Electronic Records Management Guidelines
Version 4, March 2004

State Archives Department, Minnesota Historical Society
345 Kellogg Boulevard West
Saint Paul, Minnesota, 55102-1906
651-259-3260

Shawn Rounds
Government Records Specialist
shawn.rounds@mnhs.org
651-259-3265

Robert Horton
State Archivist
robert.horton@mnhs.org
651-259-3240

The State Archives would like to acknowledge Signorelli & Associates, Inc. for writing and editing the guidelines.

Table of Contents

Introduction

Summary

You routinely create, use, and manage information electronically in your daily work as you use computers to send e-mail, create spreadsheets, publish web pages, manage databases, and create other electronic materials. Because you work for a government agency, Minnesota and federal laws mandate that you treat that information as official government records.

You probably already have a strategy to manage your paper records. With the growing pervasiveness and importance of electronic records, you should also develop a strategy to manage electronic records.

Common Questions

As you begin the process of developing an electronic records management strategy, you will find yourself asking many questions, including:

- Which Minnesota laws apply to electronic records?
- How do we use electronic records to help ensure public accountability while ensuring that not-public records are protected?
- Who is responsible for developing our electronic records management strategy?
- How do we dispose of electronic records?
- Should we manage our electronic records differently from our paper records?
- How do we know what information is an electronic record?
- Is an electronic copy of a record an acceptable substitute for the original?
- Does an electronic record have the same legal significance as a paper record?

Legal Framework

The Minnesota laws governing records management address these questions. Therefore, your understanding of existing Minnesota statutes is crucial as you begin to develop your electronic records management strategy.

Electronic records, just like paper records, are subject to specific Minnesota statutes that you must understand and comply with, including general records laws and electronic records laws.

General records laws include:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>)

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>)

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>)

Electronic records laws include:

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>]

- Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>)

Official Records Act

The Official Records Act is a general records law that mandates that “all officers and agencies” at all levels of government “shall make and preserve all records necessary to a full and accurate knowledge of their activities.” This mandate reflects a concern for accountability: since government spends public money on public services, government agencies must be accountable to citizens, government administrators, courts, the legislature, financial auditors, and to history—that is, to future generations. Under the Official Records Act, your agency’s chief administrative officer is responsible for creating and preserving government records, including electronic records. This statute also allows you to copy records to another format or storage medium and still preserve the authenticity, reliability, and legal admissibility of the record, as long as the copies are made in a trustworthy process.

Records Management Act

The Records Management Act recognizes that creating comprehensive records and preserving them forever would be an impossibly expensive burden. Instead, the Act creates a mechanism for the orderly and accountable disposition of records in the form of the Records Disposition Panel. The Act also makes the state’s Department of Administration (the Information Policy Analysis Division specifically) responsible for overseeing the records management process.

Records Disposition Panel Members

The Records Disposition Panel includes the:

- Attorney General, for expertise on the legal value of records

- Director of the Minnesota Historical Society, for expertise on the historical value of records

- Legislative Auditor (for state agencies) or State Auditor (for local agencies), for expertise on the accounting value of records

Records Disposition Panel Functions

The panel reviews, evaluates, and then approves or disapproves requests to dispose of records, to transfer records, and to establish records retention schedules. Fundamentally, the panel provides oversight, but does not initiate any actions. If your agency wants to keep records forever, then you never have to work with the panel. However, if your agency wants to do anything else legally with your records, you must submit your proposal to the panel for approval.

Minnesota Government Data Practices Act

The MGDPA assumes that government records (including electronic records) should be accessible to the public. Citizens should know what the government is doing, because the government must be accountable to the public. However, government agencies create some records that are confidential or sensitive, such as child protection records and adoption records. So, while in theory all records are presumed to be publicly accessible, many exceptions exist. Only the Minnesota state legislature defines these exceptions. Any organization, public or private, that improperly releases data covered by the act could suffer significant penalties.

Uniform Electronic Transactions Act and Electronic Signatures in Global and National Commerce

UETA and E-Sign were both enacted in 2000. Both laws intend to facilitate the use of information technology in government and business by addressing the legal obstacles that exist in a system oriented towards paper records and signatures.

The primary message of the laws is that a court may not determine that an electronic record or signature is untrustworthy simply because it is in an electronic format. A court can, though, reject electronic records and signatures because a government agency is creating, using, or managing them in an untrustworthy system or manner. One indicator of untrustworthiness would be an agency’s failure to respect the laws governing records.

Guidelines

Because these laws set forth general principles that do not always translate easily into specific technological terms, the State Archives Department of the Minnesota Historical Society has developed a series of guidelines on basic electronic records management topics within the context of these laws.

Purpose of the Guidelines

These guidelines should serve as a starting point and a guide as you review your electronic records management practices and develop an electronic records management strategy. Each set of guidelines provides an overview of key concepts within the applicable legal framework, a section containing questions to spark discussion, and an annotated list of resources to use for more detailed research. We recommend that you begin by reading the *Electronic Records Management Strategy* guidelines for a general introduction to key concepts.

Guidelines in the Series

Guidelines in the series include:

- *Electronic Records Management Strategy*. Read this set of guidelines first for basic, key concepts in electronic records management.
- *Long-Term Preservation.* Learn about the steps to developing a long-term electronic records preservation plan.
- *Metadata.* Introduce yourself to metadata, its functions, and its importance in managing electronic records. Become familiar with specific metadata standards.
- *File Naming*. Learn about the importance of including a file naming policy in your electronic records management strategy.
- *File Formats*. Review descriptions of common file formats and a summary of the issues regarding converting or migrating files.
- *Storage Facilities and Procedures*. Learn about physical storage space options and access procedures.
- *Digital Media*. Review digital media storage options (e.g., magnetic tape, optical disk) for your electronic records.
- *Electronic Document Management Systems*. Introduce yourself to electronic records issues that may arise as you seek to integrate and manage the records management process with an electronic document management system.
- *Digital Imaging*. Introduce yourself to digital imaging, its uses, and legal considerations. Review recommendations for implementing digital imaging projects.
- *E-mail Management*. Consider the issues involved in extending your electronic records management strategy to your e-mail messages.
- *Web Content Management*. Learn how to develop a policy for managing your web content that meshes with your electronic records management strategy.
- *Electronic and Digital Signatures*. Learn about the distinction between electronic and digital signatures, and the legal considerations surrounding their use.
- *Glossary*. Look up key terms in the guidelines.

Electronic Records Management Strategy

Summary

The arrival of the Information Age means that much of our history is now recorded in electronic format, including your agency's activities. Because of that, you need to develop a strategy for managing electronic records. A government agency's electronic records management strategy must conform to legal mandates, as well as reflect your preferred management practices and technological options.

Legal Framework

Your strategy must conform to the legal mandates in such areas as:

- Providing public accountability
- Distinguishing public from not-public records
- Creating records retention schedules and carrying out disposal actions
- Developing and sustaining a trustworthy process for electronic records management

Refer to the *Introduction* for more information on legal mandates, including the:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to fulfill the obligations of accountability and specifies that the medium must enable the records to be permanent. It further stipulates that you can copy a record and that the copy will be legally admissible in court.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel for an orderly disposition of records using approved records retention schedules.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that your records should be accessible to the public unless categorized as not-public by the state legislature.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

Because different stakeholders throughout an enterprise have different needs and roles in electronic records management, the development of your electronic records management strategy requires joint planning, communication, and training.

When you begin to develop your electronic records management strategy, you should aim for a policy that integrates:

- The legal framework as it applies to your agency
- All interested stakeholders (e.g., record creators, the public, information technology staff, records management staff)
- All relevant aspects of your electronic records
- Your preferred management procedures and technologies
- Long-term storage and access needs (both legal and operational)

A sound, integrated strategy reflects the relationship between records management and your operations, and ensures that you manage records in a way that supports your daily work, supports long-term operational needs, and meets your legal requirements.

Key Concepts

As you develop an electronic records management strategy, you will need to be familiar with the following key concepts:

- The State of Minnesota’s definition of a record
- Records series
- The components of an electronic record
- The records continuum
- Records management goals
- Long-term retention approaches
- General records retention schedules
- Storage options

Definition of a Record

The Records Management Act [Minnesota Statutes, Chapter 138.17] defines government records as:

> Cards, correspondence, disks, maps, memoranda, microfilms, papers, photographs, recordings, reports, tapes, writings, optical disks, other data, information, or documentary material, regardless of physical form or characteristics, storage media or conditions of use, made or received by an officer or agency of the state and an officer or agency of a county, city, town, school district, municipal subdivision or corporation or other public authority or political entity within the state pursuant to state law or in connection with the transaction of public business by an officer or agency.

In short, an official record includes all information, *regardless of format*, created or used in the course of a government business function or transaction.

The definition *excludes*:

- Library and museum material made or acquired and kept solely for reference or exhibit purposes
- Extra copies of documents maintained only for the convenience of reference
- Stock of publications and processed documents
- Bonds, coupons, or other obligation or evidence of indebtedness, the destruction or other disposition of which is governed by other laws

An *electronic record* is a record created, generated, sent, communicated, received, or stored by electronic means. Like paper records, electronic records require a long-term records management strategy.

For more information, refer to the *Preserving and Disposing of Government Records* booklet. (See the Annotated List of Resources at the end of these guidelines.)

Records Series

Your electronic records will be organized into records series. A *records series* is a set of records grouped together because they relate to a particular subject or function, or result from the same activity. All records fall into a records series, and each records series should be managed according to an appropriate records retention schedule.

By managing related records as a group, you can efficiently preserve and dispose of your records. For example, all records (regardless of format) relating to a particular committee's activity on a single issue may constitute a records series that must be preserved for ten years before disposition.

Your agency will need to organize its own records series based on its unique needs within the legal framework.

Record Components

The components of any record include:

- *Content*. Factual information in the record that documents government business
- *Context*. Information that shows how the record is related to the business of the agency and other records
- *Structure*. Technical characteristics of the record (e.g., file format, data organization, page layout, hyperlinks, headers, footnotes)

Records Continuum

Aside from reflecting your legal requirements, a successful long-term records management strategy reflects the records management continuum.

The records continuum concept reflects the idea that different stakeholders create, use, manage, and retain records, not in discrete stages, but at different points throughout the record's existence. The continuum concept recognizes that records pass through identifiable stages; however, these stages are reference points, not separate functions. In other words, a record is not simply created, passed to a records manager for short-term storage, and then passed to an archivist for long-term storage. Instead, each person's activities will have an effect on all the others in the continuum. Their roles and responsibilities should be coordinated, not organized autonomously.

The continuum concept outlines four actions that recur throughout the life of a record. These actions are:

- *Identification*. Determining what constitutes a record
- *Intellectual control*. Making decisions about the record
- *Provision of access*. Enabling users to access the records
- *Physical control*. Managing the physical location and format of the record

Each person who touches the record performs one or all of these activities. For example, the records creator, records manager, and archivist all manage the physical location of the record. Therefore, all these people should collaborate on a comprehensive and well-managed electronic records management strategy.

Records Management Goals

Although the specific strategy that your agency develops and implements will be unique, all strategies share common goals. No matter what your final strategy, the records that exist in your agency should be:

- *Trustworthy*. Trustworthy records contain information that is reliable and authentic. For more information on determining the trustworthiness of information, refer to the *Trustworthy Information Systems Handbook*. (Download information is included in the Annotated List of Resources at the end of these guidelines.) A key aspect to trustworthiness is legal admissibility, i.e. whether your records will be accepted as evidence in court.

- *Complete*. Your records should have all the information necessary to ensure their long-term usefulness. You will also need to capture and maintain the necessary metadata about your records. *Metadata* is the "data about the data" that documents the relationship of the record to your agency's activity and to other records. Metadata ensures that you can find your records. Metadata includes such elements as the record's creator, the date of creation, and the record series to which the record belongs. (For more information on metadata, refer to the *Metadata* guidelines).

- *Accessible*. You should be able to access and locate your records in a way that meets your needs and the needs of all other concerned parties. Some records may need to be immediately accessible, while others may not. As outlined in the MGDPA, records are assumed to be accessible to the public, unless categorized as not-public by the state legislature.

- *Durable*. You also want to ensure that your records are durable. In other words, they must be accessible for the designated records retention period and stored, as appropriate, "on a physical medium of a quality to ensure permanent records," as stated in the Official Records Act [Minnesota Statutes, Chapter 15.17]. For more information on records storage, refer to the following guidelines:

  - *Digital Media* for more information about digital media options available for electronic record storage

  - *Storage Facilities and Procedures* for information about the physical requirements for storing electronic records

Long-Term Retention Approaches

You have two viable, often compatible, approaches for the long-term retention of your records:

- *Conversion*. When you convert a record, you change its file format. Often, conversion takes place to make the record software independent and in a standard or open format. For example, you can convert a record created in WordPerfect by saving it as a Rich Text Format (RTF) file or to Microsoft Word. (For more information on file formats, refer to the *File Formats* guidelines.)

- *Migration*. When you migrate a record, you move it to another computer platform, storage medium, or physical format. For example, when you migrate records, you may need to migrate them to another storage medium to ensure continued accessibility. For example, if you migrate records from magnetic tapes that deteriorate, you may need to migrate the records to a compact disk to ensure continued accessibility. (For more information on storage media, refer to the *Digital Media* guidelines.)

As you consider conversion and migration, consider which media are appropriate for long-term retention. You may discover that another medium (e.g., paper or microfilm) is the best option. You may also determine that you want to combine approaches, such as converting all files to an open format and migrating them to a single platform and storage medium. (For more information on migration and conversion, refer to the *Long-Term Preservation* guidelines),

General Records Retention Schedules

Your electronic records management strategy should include records retention schedules for electronic records. A records retention schedule is a plan for the management of records listing types of records and how long they should be kept. The purpose of a records retention schedule is to serve as an on-going authorization for the management and disposition of records.

Because they have similar responsibilities and organizations, many local government entities have developed general records retention schedules for all the records commonly created by their members. General records retention schedules exist for cities, townships, school districts, counties, and courts. These general records retention schedules meet the legal requirements for each type of local agency. Your agency can adopt the general records retention schedules for your type of organization in whole, or in part, or change individual components to create a unique schedule. You may also initially choose to develop a specific schedule for your agency. However, you must submit any proposed changes to the Records Disposition Panel for approval. (For more information on the Records Disposition Panel, refer to the *Introduction*.)

Storage Options

Your options for storage include:

- *Online*. Properly designed storage in your computer system may provide full access to appropriate users. Online access means that the record is accessible immediately through your network (e.g., on your network server or on your personal computer’s hard drive). This option maintains the greatest functionality.

- *Nearline*. Nearline storage includes storage in a system that is not a direct part of your network, but that can be accessed through your it (e.g., an optical media jukebox). This option maintains a moderate amount of functionality.

- *Offline*. Offline storage refers to storage that is not accessible through your network (e.g., removable media such as magnetic tape). This option retains the least amount of functionality, while still maintaining records in an electronic format.

- *Paper or microfilm*. Printing records onto archival-quality paper or outputting them to microfilm for storage may be acceptable as long as the complete record, including all components and metadata, is included.

Key Issues to Consider

Now that you are familiar with some key concepts in electronic records management, you can use the questions below as you develop your own strategy. The careful consideration of these questions will help ensure that:

- All relevant stakeholders agree to the process and are ready to use the procedures outlined in the strategy once it is implemented

- The strategy meets your legal requirements, such as public accountability, records retention schedules, and trustworthiness

- You maximize efficiency by working with other agencies and gaining from their experience

Discussion Questions

- What legal issues do we face? Who will need access to our records (e.g., the public, other government agencies)? Do we have information that *must* be accessible to the public? Do we have information that is not-public as classified by the MGDPA that must *not* be disclosed to the public (e.g., social security numbers, adoption records)?

- Can we adopt one of the general records retention schedules, or do we need to modify or create an agency-specific records retention schedule and seek approval from the Records Disposition Panel?

- What are the roles of different groups and individuals in our organization in ensuring a coordinated process? How can we facilitate planning, communication, and cooperation among all individuals who create and use the electronic records? What level of control should different individuals and groups have?

- Can we cooperate with other government agencies to streamline the process and save money or time?

- What best practices can we identify and apply to our own situation?

- What is the life cycle of our data? When should we capture records? How can we describe our records continuum? At which phases along our continuum do we need to actively manage the record? Would we benefit from developing a model of our operational process to aid in this discussion?

- How will we ensure long-term preservation and access? What are our requirements under the law?

- What are our options for long-term retention? What are the advantages of each option? How would each option work in our particular situation? What is our budget?

- What technological resources do we have available? How much of our chosen process can we or should we automate?

- What sort of appraisal process will we use to determine which records to keep? How will we ensure that this process identifies all records as defined by the law?

- What staff training do we need to ensure the staff complies with the new procedures and policies?

- What elements of the electronic records do we need to keep (e.g., text content only, graphical appearance, interactivity)?

- What metadata do we need to collect and preserve?

Annotated List of Resources

Primary Resources

Hunter, G. S. “Storage, Handling, and Preservation Best Practices.” In *Preserving Digital Information, A How-To-Do-It Manual.* New York: Neal-Schuman Publishers, Inc., 2000: 53–93.

> *These hands-on recommendations provide practical information for electronic records storage, handling, and preservation. Topics covered include useful information on the deterioration of magnetic media, recommended storage conditions, proper care and handling, file formats (including advantages and disadvantages of different formats), and other best practices.*

Minnesota Historical Society, State Archives Department. *Preserving and Disposing of Government Records.* St. Paul: Minnesota Historical Society, May 2008. <http://www.mnhs.org/preserve/records/docs_pdfs/PandD_may2008.pdf>

> *Developed for Minnesota government agencies, this overview of the basic principles of records management includes chapters on defining a government record, taking inventory of your records, developing records retention schedules, preserving archival records, disposing of records, and setting up a records storage area. A list of resources for more information is included, as well as information about applicable state law regarding electronic records management. Originally published by the Minnesota Department of Administration in July 2000, the guide was updated jointly by the Minnesota Historical Society and the Minnesota Government Records and Information Network (MNGRIN) in 2008.*

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002. <http://www.mnhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.*

Stephens, D. O. and R. C. Wallace. “Electronic Records Retention: Fourteen Basic Principles.” *The Information Management Journal* 34 (October 2000): 38–52.

> *Providing a brief, but complete, overview of the basic principles of electronic records management, this article also contains practical guidelines for developing an electronic records management strategy.*

Additional Resources

Barata K., P. Cain, R. Routledge. *Principles and Practices in Managing Financial Records: A Reference Model and Assessment Tool*. London: International Records Management Trust,

Rights and Records Institute, 2001.
<http://www.irmt.org/Images/documents/assessment%20tools/mfsr.pdf>

Of particular interest to the public sector, this handbook provides an overview of international best practices in the management of electronic financial records.

Bill Number S-761. Washington, D.C.: Library of Congress, 2001.
<http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>

This site provides the results of a search for E-Sign legislation in the Thomas database of legislative information on the Internet. The site lists five versions of the bill (including the final enrolled bill) for the 106th congress (1999–2000). The site provides a downloadable file of the bill, plus links to other information about the bill in the Congressional Record and committee reports.

COOL, Conservation OnLine
<http://palimpsest.stanford.edu>

A compilation of materials from other sources about electronic conservation, this web site includes links to resources on disaster recovery, electronic media, electronic formats, and storage environments.

International Council on Archives, Committee on Electronic Records. *Guide for Managing Electronic Records from an Archival Perspective*. Paris: International Council on Archives, 1997.
<http://www.ica.org/sites/default/files/ICA%20Study%208%20guide_eng_0.pdf>

This handbook provides a comprehensive overview of electronic records management from an archival perspective. It provides useful information on key concepts, such as life-cycle management, legal issues, technological issues, and implementation tactics for all readers.

InterPARES Project
<http://interpares.org>

This web site is a comprehensive resource for information about the InterPARES Project. This project is an international research initiative to develop a theory and methods for permanent electronic records preservation. The site includes white papers, links to additional resources, presentations, and workshop listings.

Public Records Office of the United Kingdom. *Records Management: Electronic Records.*
<http://www.pro.gov.uk/recordsmanagement/erecords/default.htm>

Published by the Public Records Office of the United Kingdom, this site provides a wide range of information, including downloadable documents on the management, appraisal, and preservation of electronic records; how to incorporate a policy on electronic records *management; and toolkits for compiling an inventory of electronic records collections.*

Long-Term Preservation

Summary

During the course of routine business, your agency generates thousands upon thousands of electronic records, from e-mail to web pages to complex e-government transactions. Most are useful for only a short period of time, but some you may need to keep permanently. For those records, you will need to implement a well-considered, well-documented plan for their preservation in order to ensure that they remain trustworthy and useful over time. Tools such as migration, conversion, metadata, and eXtensible Markup Language (XML) will help you not only preserve your records, but also realize their full value.

Legal Framework

For more information on the legal framework to consider when developing a preservation plan for your records, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook*. Also review the requirements of:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to maintain their accountability and specifies that the medium must enable the records to be permanent. The Official Records Act further stipulates that you can copy a record and that the copy, if trustworthy, will be legally admissible in court.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records using approved records retention schedules. Coordinate your records retention schedules with your preservation plan to help ensure that you store and dispose of records in accordance with the Records Management Act.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that government records should be accessible to the public unless categorized as not-public by the state legislature. You must be able to provide access to the stored public records, yet prevent unauthorized access to not-public records.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of legal admissibility of electronic records created in a trustworthy manner and the application of a paper-oriented legal system to electronic records.

- Information and Communications Technology Policy [Minnesota Statutes, Chapter 16E.04] (available at: <http://www.revisor.leg.state.mn.us/stats/16E/>), which mandates state agency compliance with Minnesota's enterprise technical architecture "to ensure that individual agency information systems complement and do not needlessly duplicate or conflict with the systems of other agencies. . . . [and to] promote the most efficient and cost-effective method of producing and storing data for or sharing data between those agencies." Section 16E.07 establishes the North Star portal as the state's official online government information service with the idea that "the greatest possible access to certain government information and data is essential to allow citizens to participate fully in a democratic system of government."

Key Concepts

The value of your information justifies your investment in information technology. There is no point to an agency investing large sums in hardware and software if it cannot preserve the use-value of the information it creates, exchanges, and stores. In the short-term, this is often not a problem. But, over time, it will be. As technology changes, hardware and software will become obsolete, and then you might face some hard choices. The challenge is to preserve the usefulness and trustworthiness of your information in an efficient and cost-effective way.

Any preservation plan for electronic records must take into account the changes in hardware and software, the limitations of storage media, and the potential use-value of your information. As you begin exploring your options, you will need to be familiar with the following:

- Needs analysis
- Physical storage options
- File format options
- Digital preservation techniques
- E-government and collaboration

Needs Analysis

As a first step in developing your preservation plan, you should do a needs analysis to help guide your decisions. While the complexity of such an analysis will vary from situation to situation, these basic components should always be included.

First, you need to understand the value of your information. The value of your information will justify your investment in technology, over the short- and the long-term. Minnesota's enterprise technical architecture notes that information is the state's most important asset. But all information is not created equal; some has much more value than others. Some of your information, as records, will have legal and evidentiary significance and may well demand special attention. Most of the information you want to preserve will be important to your agency's mission or, increasingly, to the business of other agencies as well. As e-government develops in complexity and sophistication, more and more agencies will be expected to work within the framework of a common technological architecture and to share the information they create.

The practical side of understanding the value of your records is determining their retention requirements. How long do you really need to keep them? Why are you keeping them? Do they have to be kept in electronic format or is there another, more cost-effective option for long-term storage? For instance, a word processing document might be printed and kept as a paper record without losing any of its value. In contrast, printing a web page means a significant loss of information and functionality.

It is also important to ascertain if access to certain data in your records is restricted by statute. The state's Government Data Practices Act and some federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), will determine if data needs to be protected as confidential or non-public. If it does, then you will need to ensure that your long-term storage and access policies account for those obligations.

In the broadest sense, the demands governing the access and use of your records will determine what preservation options are most appropriate and will dictate the metadata you should create and store along with the records. Metadata is the "data about the data," that allows you to manage, find, and evaluate your information over time. Minnesota's enterprise technical architecture includes metadata standards for GIS data, web content management, and recordkeeping. There are a number of international standards that are pertinent as well. While all-important for the long-term preservation of data, metadata takes on additional significance when you share your information because others must understand the information's structure and content in order to put it to fullest use. For more information about metadata, refer to the *Metadata* guideline in this series.

Physical Storage Options

As mentioned, choosing the most appropriate storage option for your situation will depend upon your records' access requirements. There are basically three options available to you:

- *Online storage*. Records are kept on a server or hard drive and are immediately available for use over a network. This option is best for records that must be accessed frequently.

- *Nearline storage*. Records are stored on media such as optical disks in jukeboxes or tapes in automated libraries which are attached to a network. Because retrieval is slower than with online storage, this option is most appropriate for records that are accessed occasionally.

- *Offline storage*. Records are stored on removable media and must be manually retrieved. This option provides the slowest access and should be used for records that are only rarely needed.

If you choose nearline or offline storage, you will need to consider what media will best suit your needs. To do this, you should start by analyzing your current and projected volume of stored records, along with the size of the files themselves and any associated metadata. Also take into account any security requirements, such as viewing, use, and modification restrictions.

Different media have different storage characteristics. For instance, with CD-R, DVD-R, and DVD+R disks, data can be recorded one time only, after which the media becomes read-only. This provides protection for your records against intentional or unintentional tampering. CD-RW, DVD-RW, DVD+RW, and DVD-RAM can all be written to multiple times, although at the cost of diminished life span and the risk of possible loss or alteration of the contents. CDs can generally store up to 800 MB of data, while DVDs can store several gigabytes. Magnetic tape is an alternative to optical disk, with capacity up to several gigabytes, although retrieval is much slower since it is a sequential-access rather than random-access medium. Tapes are most often used for offline storage and backups.

Life spans also differ among media types. Under optimal storage and use conditions, optical disks and magnetic tapes will generally give reliable service for anywhere between 5 and 20 years. Under normal conditions, however, life expectancies are probably significantly shorter. For more information on media types, refer to the *Digital Media* guideline in this series.

File Format Options

Most records are created using specific, proprietary software applications. Over time, these applications will be upgraded or be phased out altogether. Because upgraded applications may or may not be able to read files created with previous versions, backward compatibility is not a given and cannot be counted on as a preservation tool. Maintaining the software on your own is an option, but over and above the question of costs, that carries the risk the software will fail in time, leaving you with no way to access your records. One common alternative is continually to convert your files from version to version and format to format as your software environment changes.

While non-proprietary formats are the ideal for the long-term preservation of files, they are few in number and each has its limitations. ASCII or plain text will capture data in the lowest common denominator of formats, losing structure and functions in the process. Rich Text Format (RTF) is a Microsoft format, although it is supported by a variety of vendors and software applications. Portable Document Format (PDF), a popular choice for file sharing and storage, is an Adobe product. Because Adobe makes PDF’s specifications publicly available, many believe that it is an open standard when, in fact, the company is under no obligation to continue this practice into the future. Furthermore, PDF has a problem with backward compatibility, with newer versions often incorrectly rendering files created with older ones. To address these problems, an archival version, currently referred to as PDF/A, has been developed and is under consideration as a potential ISO standard.

For long-term preservation and use, eXtensible Markup Language (XML) is currently the optimum choice of formats. An international standard since 1998, XML is both a file format and a text-based, self-describing, human-readable markup language that is independent of hardware and operating systems. Because it is infrastructure-independent, XML is one of the best solutions for re-purposing the content of your records and/or sharing them with others. Proper use of XML requires a certain amount of planning and up-front commitment of money and time, but its structured nature makes it suitable for automation and will allow you to more easily take advantage of whatever new open formats will follow in the future. For more information on file formats, refer to the *File Formats* guideline in this series.

Digital Preservation Techniques

There are several approaches, some more practical than others, to ensure that electronic records remain useful over time. One is to save all of the hardware, software, and documentation needed to support the records. Known as the "computer museum" approach, it is not very realistic on a large scale because, given how rapidly hardware and software environments change, it means storing and maintaining huge quantities of outdated equipment with no assurance that any of it will work when needed.

Emulation has a similarly antiquarian flavor. Emulator programs simulate the behavior, look, and feel of other programs, thus preserving the functionality of the records in their original format without the necessity of saving the original equipment and software. However, emulation has so far proven more attractive in theory than in practice. There are few examples of success using this approach, and costs have proven high. It has a further limitation in that, at best, emulation simply reproduces earlier, less sophisticated versions of an application. Given all the expenses of technology, it seems problematic to limit the value of information by preserving it in a static framework.

Encapsulation is a third approach to preservation. It involves combining the object to be preserved with all of the necessary details of how to interpret it within a wrapper or package, all possibly formatted in XML. While appealing in its comprehensiveness, encapsulation has several drawbacks: file sizes are large because of all of the included information; format specifications must be determined; the encapsulated records must somehow be generated, usually separate from the act of record creation; and the encapsulated records must still be migrated over time.

The most common approach to preserving electronic records involves a combination of two other techniques: migration and conversion. Migration is the process of moving files to new media (also know as "refreshing") or computer platforms in order to maintain their value. Conversion entails changing files from one format from one to another and may involve moving from a proprietary format, such as Microsoft Word, to a non-proprietary one such as a plain text file or XML. To avoid losing data in the process, you should perform initial tests and analysis to determine exactly what changes will occur and whether they are acceptable. With both migration and conversion, special attention must be paid to also maintaining the accessibility of any associated metadata. When properly planned and executed, the migration and conversion approach probably represents the easiest and most cost-effective preservation method available today.

E-Government and Collaboration

The State of Minnesota's e-government framework should influence your preservation plans. The long-term preservation of records will demand a variety of investments and decisions that will involve time, staff, technology, and specialized expertise. Practically speaking, the state probably cannot afford to have every agency make all those investments independently. Similarly, no agency, even with the best of intentions, can consistently make all those decisions correctly. Finding effective and economic solutions means working together.

The state's enterprise technical architecture reflects that. In order to facilitate the development of e-government, the architecture identifies a series of issues, approaches, and standards that will make your agency's investments in information technology more likely to succeed. At the same time, these also will facilitate the long-term preservation of digital resources through sharing services and solutions. In developing your preservation strategy, start by looking at what other agencies are doing and what you can learn from their experiences.

Key Issues to Consider

The foundation of your preservation plan should be your needs analysis, as well as an analysis of the costs, benefits, and risks involved with each of the options you are studying. Your records management, information technology, and legal staff should all be involved in the process to make sure your plan meets your business requirements and fits in with your general electronic records management strategy. Be sure to document your decision-making process in addition to your choices and plans for implementation.

At the minimum, your preservation plan should include the following items:

- Rationale and requirements for your preservation program.
- List of relevant records series and their retention and access requirements.
- Explanation of the selected preservation technique(s), including schedules for preservation actions, quality assurance testing, backups, etc. and instructions for documentation.
- Pointer to a business continuity or disaster recovery plan.

Once completed, your preservation plan should not gather dust on a shelf. Rather, it should be a reference document for all preservation activities, and it should be kept up to date as your situation changes (e.g., changes in use needs, hardware, software, media, security/access requirements, retention periods, legal mandates).

Discussion Questions

As you move from your needs analysis to the development of your preservation plan, you will face many choices. These are just a few of the questions you should ask during the process.

- How long do we need to keep these records? What will be the costs associated with such preservation tasks as migration and conversion over time?

- What best practices can we identify and apply to our situation? Can we cooperate with other agencies or organizations to share expertise or save money?

- Do we need to keep the records in electronic format or is another format, such as paper or microfilm, more appropriate? How much functionality do we need to retain over time?

- How often are these records accessed? What is the best storage solution (e.g., online, nearline, offline)?

- What is the most appropriate storage media for the records? How will we ensure that we retain the hardware necessary to handle the media? What documentation should we collect and maintain regarding the media and hardware?

- How will we ensure that the content of the records is accessible and readable over time? Is the format and necessary software proprietary or non-proprietary? What documentation should we collect and maintain regarding format and software?

- How will we perform periodic quality assurance checks to ensure accessibility and trustworthiness over time? How will we document these checks?

- What indexing and metadata schemes should we employ to ensure that the records can be easily located and evaluated for use?

- How will these records be used? Will they be shared with others inside our organization? Outside? Would XML enhance the use-value of the records?

- Have the records been compressed or encrypted? If so, how does this fit into our management plan?

- Are there data access issues that require special security measures?

- What hardware and software configurations are we moving to in the foreseeable future? How do these records fit in with that plan?

- What staff training is necessary to ensure compliance with the preservation plan?

Annotated List of Resources

Primary Resources

Beyers, Fred R. *Information Technology: Care and Handling for the Preservation of CDs and DVDs – A Guide for Librarians and Archivists*. NIST Special Publication 500-252. Gaithersburg, MD: National Institute of Standards and Technology; Washington, D.C.: Council on Library and Information Resources. October 2003. <http://www.foray.com/images/pdfs/CDandDVDCareandHandlingGuide.pdf>

> *This guide discusses the physical characteristics of various optical media, as well as methods for their proper care and handling to ensure longest possible use in any given environment. A useful glossary is included.*

Lawrence, Gregory W., William R. Kehoe, Oya Y. Rieger, William H. Walters, and Anne R. Kenney. *Risk Management of Digital Information: A File Format Investigation*. Washington, D.C.: Council on Library and Information Resources. June 2000. <http://www.clir.org/pubs/reports/pub93/pub93.pdf>

> *This publication offers detailed guidance on migration (which is defined to include conversion) as a preservation technique through a risk assessment process. A useful workbook is provided to assist users in applying quantitative risk assessment measurements to their own environment.*

Lee, Kyong-Ho, Oliver Slatterly, Richang Lu, Xiao Tang, and Victor McCrary. "The State of the Art and Practice in Digital Preservation." *Journal of Research of the National Institute of Standards and Technology*. 107(January-February 2002): 93-106. <http://nvl.nist.gov/pub/nistpubs/jres/107/1/cnt107-1.htm>

> *This paper provides a concise survey of a variety of preservation techniques for digital resources, including migration, emulation, encapsulation, and the use of eXtensible Markup Language (XML), as well as some project case studies.*

Minnesota Department of Administration, Office of Enterprise Technology. *Minnesota Enterprise Technical Architecture.* Version 2.02, 2006.
<http://www.oet.state.mn.us/>

> *The Minnesota Office of Enterprise Technology (OET) is charged with establishing and maintaining a state information architecture as specified in Minnesota Statue, Chapter 16E.04 Subdivision 2. According to the OET, "This technical architecture is established to describe technology components of the State's information infrastructure and their individual principles, practices and standards that are to be used to guide the development and delivery of all information systems services. The architecture will provide a reference so that various groups of government IT professionals have a consistent view of the information systems infrastructure and the methods that they employ to develop and deliver information systems services." Chapter 4, Data and Records Management, describes the framework for managing information resources, as well as the standards and guidelines that apply.*

World Wide Web Consortium (W3C). Extensible Markup Language (XML).
<http://www.w3.org/XML/>

> *The W3C is the international body responsible for the development and ongoing refinement of the XML family of standards. This site provides links to the specification itself, as well as pointers to working groups and other resources.*

Additional Resources

Minnesota Historical Society, State Archives Department. *Preserving and Disposing of Government Records.* St. Paul: Minnesota Historical Society, May 2008.
<http://www.mnhs.org/preserve/records/docs_pdfs/PandD_may2008.pdf>

> *Developed for Minnesota government agencies, this overview of the basic principles of records management includes chapters on defining a government record, taking inventory of your records, developing records retention schedules, preserving archival records, disposing of records, and setting up a records storage area. A list of resources for more information is included, as well as information about applicable state law regarding electronic records management. Originally published by the Minnesota Department of Administration in July 2000, the guide was updated jointly by the Minnesota Historical Society and the Minnesota Government Records and Information Network (MNGRIN) in 2008.*

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook.* Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy*

information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.

Metadata

Summary

Metadata is usually defined as "data about data." Metadata allows users to locate and evaluate data without each person having to discover it anew with every use. Its basic elements are a structured format and a controlled vocabulary, which together allow for a precise and comprehensible description of content, location, and value.

While the term itself might sound new and trendy, the concept it describes is not. In some fashion, metadata has always been with us, apparent in everything from program listings in *TV Guide* to the nutritional information on the back of a cereal box. For government records, the familiar forms of metadata are the recordkeeping metadata standard and the records retention schedule.

Anyone who has suffered the exercise in irrelevance offered by an Internet search engine will appreciate the value of precise metadata. Because information in a digital format is only legible through the use of intermediary hardware and software, the role of metadata in information technology is fundamentally important. In any system, given the volume of information it contains, the uses to which it can be put, and the costs involved, metadata is the basic tool for efficiency and effectiveness.

Whatever you want to do with the information (e.g., protect its confidentiality, present it as evidence, provide citizens access to it, broadcast it, share it, preserve it, destroy it) will be feasible only if you and your partners can understand and rely upon the metadata describing it. Using metadata effectively means understanding and applying the standards appropriate to your needs.

Key Concepts

To understand, create, and use metadata effectively, you will need to know more about:

- Metadata functions
- Legal needs and statutory mandates
- Metadata and technology
- Metadata standards

Metadata Functions

Government agencies routinely use metadata to fulfill a variety of functions, but the primary uses are for:

- Legal and statutory reasons (e.g., to satisfy records management laws and the rules of evidence)

- Technological reasons (e.g., to design and document systems)

- Operational or administrative reasons (e.g., to document decisions and establish accountability)

- Service to citizens, agency staff, and others (e.g., to locate and share information)

In all of these cases, metadata standards will be effective only if they rely on a structured format and controlled vocabulary. “Structured format” means the metadata is defined in terms of specific, standardized elements or fields. For example, a library catalog entry for a book will identify its author, title, subject(s), and location, among other things. Unless all the elements are there, users will not be able to evaluate the metadata; they won’t be able to answer the question “Is this the book I want?”

“Controlled vocabulary” means that there is a standard as well for the content of the elements. For example, the nutritional information on the back of a box of cereal is often defined in terms of weight per serving. We know what “sugar: three grams” means. It refers to a standard unit of measurement that allows us to compare the sugar content of one cereal to that of another. But if the box read “just the way you like it” or “pretty sweet,” that would mean different things to different people. We couldn’t compare a subjective review like that to what’s on the back of another box of cereal.

To work effectively, the elements and components of metadata should have an accepted, precise meaning that reflects a common understanding among its creators and its users. That allows for evaluation and comparison, for selecting the information you want from all the information available.

Legal Needs and Statutory Mandates

Because you are part of a government entity, you need to pay particular attention to metadata’s value to help you achieve basic legal needs and meet statutory mandates.

For example, Minnesota’s Records Management Act mandates that government agencies cannot dispose of records without the approval of the state’s Records Disposition Panel. The only way to get that approval is to describe the records: what they are, where they are, what their significance is, and how they should be disposed. All that information is metadata. In the records management process, metadata usually takes two forms, either a records retention schedule or an Application for Authority to Dispose of Records form (PR-1).

Similarly, the Minnesota Government Data Practices Act classifies data under nine different categories which specify how, when, or if the public may gain access to government data. You cannot guess what level of access or security to provide just by looking at the data itself. You need some additional information – some metadata – in order to follow the letter of the law.

These are some of the laws most pertinent to the use of metadata:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must create and keep records in order to be accountable for their actions and decisions.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which creates the Records Disposition Panel and establishes the records management process for government records.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that your records should be accessible to the public unless categorized as not-public by the state legislature.

The metadata requirements of all of these statutes are encompassed in the state's Recordkeeping Metadata Standard. For more information on the legal framework you must consider when dealing with government records, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook.*

Metadata and Information Technology

Metadata is useful for the management of information in any storage format, paper or digital. But it is critically important for information in a digital format because that is only legible through the use of intermediary hardware and software. We can open up a book or even hold microfilm up to a light to determine what it says. But we can't just look at a CD and say what's on it. We cannot possibly hope to locate, evaluate, or use all the files on a single PC, let alone the Internet, without metadata.

If information technology makes metadata necessary, it's information technology that makes metadata useful. Special software applications, such as TagGen, make the creation of standardized metadata simpler. Databases store and provide access to metadata. Most software applications automatically create metadata and associate it with files. One example is the header and routing information that accompany an e-mail message. Another is the set of properties created with every Microsoft Word document; certain elements such as the title, author, file size, etc., are automatically created, but other elements can be customized and created manually. Normally, some combination of automatically and manually created information is best for precise and practical metadata.

Most important, metadata can inform business rules and software code that transforms it into "executable knowledge." For example, metadata can be used for batch processing of files. A date element is critical to records management, as most record retention schedules are keyed to a record's date of creation. Metadata in more sophisticated data formats, such as eXtensible Markup Language (XML), allow for extraction, use, and calculation based on specific components of a metadata record.

Metadata Standards

To work effectively, metadata has to be precise and comprehensible. The entire community of creators and users has to understand what it means. There is a variety of metadata standards in use across the world, but there are three principal standards in general use in Minnesota government today. Minnesota's Office of Enterprise Technology (http://www.oet.state.mn.us/) recommends the following standards in its enterprise architecture:

- Minnesota Metadata Guidelines - Dublin Core
- Minnesota Geographic Metadata Guidelines
- Minnesota Recordkeeping Metadata Standard

Minnesota Metadata Guidelines - Dublin Core (MMG-DC)

The *Dublin Core* is a metadata standard with fifteen elements that is an official international standard (NISO Standard Z39.85; ISO Standard 15836). It was designed principally by the library and archives community, and its primary application is to describe information resources, particularly web content. When you use the search engine on the state’s North Star site, Dublin Core metadata helps you find exactly what you’re looking for.

The MMG-DC set includes these elements:

- *Title*. The name of the resource given by the creator or publisher.

- *Subject*. The topic of the resource.

- *Description*. A short, text description of the resource’s contents.

- *Creator*. The name of the person who created the resource.

- *Publisher*. The name of the entity that published the resource. Note that the publisher is not the person who posted the resource to the web site, but the entity responsible for the publication of the resource, such as your agency.

- *Contributor*. Someone aside from the creator who made a significant contribution to the resource.

- *Date*. Either the creation date or the publication date. Your agency will need to determine which date to use.

- *Resource Type*. The category the resource belongs to, such as committee minutes, press release, or report.

- *Format*. The file format of the resource. For more information on file formats, refer to the *File Formats* guidelines.

- *Identifier*. A text string or number unique to the resource, such as a URL or other formal name. See the *File Naming* guidelines for more information on naming web site files for longevity and ease of use.

- *Relation*. An element that refers to related resources.

- *Source*. Information about the source from which the current resource is derived (e.g., an abstract of a report).

- *Rights Management*. A text statement regarding copyright and use permission.

- *Language*. The language used in the resource (e.g., English, Spanish).

- *Coverage*. Either geographic (e.g., Minnesota) or temporal (e.g., the years 2000–2001).

To populate these elements and to describe web content, the State of Minnesota uses an established and maintained set of terms along with the MMG-DC. Information on the Legislative Indexing Vocabulary is available online, at <http://bridges.state.mn.us>. The State also has a license to use a specific software application, TagGen, as a tool for the creation or capture of metadata. It is available free to Minnesota government agencies. Information on using and acquiring TagGen is also online, at <http://bridges.state.mn.us>, along with an instructional manual, the *Best Practices Guidelines for Web Metadata*.

Minnesota Geographic Metadata Guidelines

The *Minnesota Geographic Metadata Guidelines* provide a common approach for documenting all types of geographic data. They have been designed to be straightforward, intuitive, and complete. The guidelines are based on a standard developed by the Federal Geographic Data Committee in 1993: *The Content Standards for Digital Geospatial Metadata*. In developing the *Minnesota Geographic Metadata Guidelines*, the Standards Committee of the Minnesota Governor’s Council on Geographic Information created a streamlined implementation of the federal standard, while retaining the essence of its original content. Information about the guidelines is available at <http://www.gis.state.mn.us/stds/metadata.htm>

The Minnesota Geographic Metadata Guidelines includes a number of metadata elements, arranged in seven sections:

- *Identification Information*

- *Data Quality Information*

- *Spatial Data Organization Information*

- *Spatial Reference Information*

- *Entity and Attribute Information*
- *Distribution Information*

- *Metadata Reference Information*

Minnesota Recordkeeping Metadata Standard

The *Minnesota Recordkeeping Metadata Standard* is designed to support the accountability of government and the proper use of government records as mandated by law. It is based on the Dublin Core, and its fields can be easily mapped to the Minnesota Geographic Metadata Guidelines.

The standard consists of twenty elements, ten of which are mandatory and ten optional. In addition, many of these elements contain a number of sub-elements, some mandatory and some optional. To ensure compatibility across metadata sets, six of the ten mandatory elements have direct counterparts both in the Dublin Core and the geographic metadata standards. Overall, the recordkeeping metadata elements are:

- *Agent*. An agency or organizational unit that is responsible for some action on or usage of a record, or an individual who performs some action on a record, or who uses a record in some way.

- *Rights Management*. Legislation, policies, and caveats that govern or restrict access to or use of records.

- *Title*. The names given to the record.

- *Subject*. The subject matter or topic of a record.

- *Description*. An account, in free text prose, of the content and/or purpose of the record.

- *Language*. The language of the content of the record.

- *Relation*. A link between one record item and another, between various aggregations of records, or a link between a record and another information resource.

- *Coverage*. The jurisdictional, spatial, and/or temporal characteristics of the content of the record.

- *Function*. The general or agency-specific business function(s) and activities that are documented by the record.

- *Date*. The dates and times at which such fundamental recordkeeping actions as of the record's or records series' creation and transaction occur.

- *Type*. The recognized form or genre a record takes, which governs its internal structure.
- *Aggregation Level*. The level at which the record(s) is/are being described and controlled or the level of aggregation of the unit of description.

- *Format*. The logical form (content medium and data format) and physical form (storage medium and extent) of the record.

- *Record Identifier*. A unique code for the record.

- *Management History*. The dates and descriptions of all records management actions performed on a record from its registration into a recordkeeping system until its disposal.

- *Use History*. The dates and descriptions of both legal and illegal attempts to access and use a record, from the time of its registration into a recordkeeping system until its disposal.

- *Preservation History*. The dates and descriptions of all actions performed on a record after its registration into a recordkeeping system which ensure that the record remains readable and accessible for as long as it has value to the agency and to the community at large.

- *Location.* The current (physical or system) location of the record or details about where the record usually resides.

- *Disposal*. Information about policies and conditions that pertain to or control the authorized disposal of records or information about the current retention schedule and disposal actions to which the record is subject.

- *Mandate*. A source of recordkeeping requirements. For example, a piece of legislation, formal directive, policy, standard, guideline, set of procedures, or community expectation which (explicitly or implicitly) imposes a requirement to create, keep, dispose of, or control access to and use of a record.

Key Issues to Consider

Now that you are familiar with some of the basic concepts and types of metadata, you can consider some of the issues that have to be addressed in order to use metadata effectively. The most important are:

- Audiences: Most people who rely on metadata are unaware they're using it or even that it exists. Nevertheless, when you create metadata, you have to be aware of the audiences for your information in order to determine the appropriate standards and approaches. To make your decisions, you should know which information resources your audiences use, which questions they ask, and what their level of expertise is.

- Partnerships: To increase the value of both metadata and the information it describes, you need to work with other creators, custodians, and users of information. If you agree on metadata standards, tools, and practices in collaboration with others, you will create a much more beneficial information management program for your whole organization.

- Implementation: Selecting a standard is a good first step. Putting it into practice is a more useful and difficult one. Creating and maintaining metadata over time will demand attention, resources, and staff. You will get a good return on that investment if you keep in mind your legal mandates, your business processes, and your customers as you choose what standards and practices are most appropriate for you.

- Education: One critical element of a practical metadata program to keep in mind is education. You will need to know about what others are doing with the standards, the tools, and the uses of metadata. As these change, you will need to keep up with those developments.

- Promotion: To promote the understanding, use, and creation of metadata, as well as to ensure that there are enough resources to support a metadata program, it is important to draw people's attention to metadata and its importance. The State of Minnesota's Information Policy Council supports a metadata awareness program designed by the Land Management Information Center and the State Archives Department of the Minnesota Historical Society. The program promotes reliable and standardized metadata with an educational resource online and a symbol:

  When you see this symbol, you are looking at information that is described by metadata created according to a recognized standard. On a web page, the symbol will act as a hot link to a page describing the value and uses of metadata and offering information about specific metadata standards used in Minnesota

Discussion Questions

- What are the business functions your metadata is supposed to fulfill?

- Who is the audience for your metadata? What are their needs?

- Does your agency have an information and/or technical architecture? What metadata standards does it recommend?

- Are your software applications creating metadata?

- What are your legal needs? Does your agency have a records management or data practices office?

- Do the managers and resource allocators in your agency support a metadata program? Have you made a business case to them?

- Are the offices or departments of your agency already creating metadata? Are they using different standards?

- What are the metadata standards pertinent to your profession or business functions?

Annotated List of Resources

Primary Resources

Dublin Core Metadata Initiative
<http://dublincore.org>

> *The Dublin Core Metadata Initiative is the official site for the Dublin Core (DC) project. The fifteen-element metadata standard is the product of a number of workshops that began in 1995 and is now an official international standard (NISO Standard Z39.85; ISO Standard 15836). Intended to serve users in a flexible manner, the elements are all optional, repeatable, and labeled with descriptive names. Metadata generated from this scheme may be represented in a number of ways (e.g., HTML, RDF) for use on the Internet.*

Minnesota Land Management Information Center (LMIC)
<http://www.lmic.state.mn.us>

> *LMIC, a division of the Office of Strategic and Long-Range Planning (Minnesota Planning), is charged with coordinating the "effective use of digital geographic data to support public policy and government operations" in the state. As a member of the GIS Standards Committee of the Minnesota Governor's Council on Geographic Information, LMIC helped develop a standard format for GIS metadata (the Minnesota Geographic Metadata Guidelines) based upon the federal model of the Content Standard for Digital Geospatial Metadata. LMIC makes available software (DataLogr) to aid data holders in recording their metadata in conformance with the Minnesota guidelines. By arrangement, LMIC offers project assistance and research- and technology-related services.*
>
> *Featured links at the LMIC site include access to 2000 Census data through Datanet and information about the activities of the Governor's Council on Geographic Information. Additionally, the Minnesota Geographic Data Clearinghouse provides a collection of resources to help find, access and use geospatial data about Minnesota regardless of source. The Clearinghouse includes: the Minnesota Geographic Data Catalog, providing information about data holdings at LMIC as well as other state and federal agencies; LMIC's metadata index, containing detailed information on over 120 data sets accessible through the agency; and the GeoGateway, a search engine that integrates access to over 300 data sets served by Minnesota organizations and over 2500 data sets focused on the geography of Minnesota. The GeoGateway assists users in locating data sets specific to the state and surrounding region by searching metadata based on user-defined criteria, including keywords, temporal considerations and geographic extent and source.*

Minnesota Department of Natural Resources. *Best Practice Guidelines for Web Metadata*.
<http://bridges.state.mn.us/bestprac/index.html>

> *Multiple documents and downloads are available on this web site, including guidelines on how to use the Dublin Core Metadata Element Set as part of the process of archiving web content and a description of each element's purpose and method of creation. The site*

also offers a bibliography, a training manual on applying the Dublin Core metadata set, background reports, and information about downloading the TagGen tool.

Minnesota Department of Natural Resources. *Bridges: Minnesota's Gateway to Environmental Information*.
<http://bridges.state.mn.us>

The Bridges project represented a collaboration between Minnesota's environmental agencies with the goal of providing easy access to their electronic resources such as web pages, PDF documents, databases, and geographic data. Resources were cataloged using the Dublin Core metadata scheme and are located through a simple cross-agency search engine (the Inktomi-powered North Star search at the state's main portal). Although the project was completed in July 2000, the web site still offers a number of resources to visitors, including best practice guidelines for web metadata, information on metadata tools, project reports, as well as links to participating agencies, other regional and federal environmental sites, and the Minnesota Governor's Council on Geographic Information.

Minnesota Department of Natural Resources. *GIS Data Deli*
<http://deli.dnr.state.mn.us>

The GIS Data Deli site is a service of the Minnesota Department of Natural Resources. Visitors may download raw spatial data pertaining to the state for use with GIS-specific software, image processing systems, or traditional databases; no online map composition or viewing is possible. Users capture the data through a process involving specifying geographic areas, layers and data elements of interest. Detailed metadata conforming to the Minnesota Geographic Metadata Guidelines is available for each layer.

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.

Minnesota Recordkeeping Metadata Standard (Minnesota Office of Enterprise Technology Standard IRM 20)
<http://www.mnhs.org/preserve/records/metadatastandard.html>

The Minnesota Recordkeeping Metadata Standard was developed to facilitate records management by government entities at any level of government. It shares many of its elements with other metadata standards, such as the Dublin Core and the Minnesota

Geographic Metadata Guidelines set, but goes further to address such issues as access restrictions, data practices, and records retention and disposition, thereby enabling the practical implementation of statutory mandates for records management. The standard is comprised of twenty elements, ten of which are mandatory.

Additional Resources

Federal Geographic Data Committee (FGDC). *Metadata.*
<http://www.fgdc.gov/fgdc/fgdc.html> and <http://fgdc.er.usgs.gov/metadata/metadata.html>

This site is sponsored by the FGDC, which is made up of several federal agencies. Working with such partners as state and local governments, the academic community, and industry, the FGDC is supervising the development of the National Spatial Data Infrastructure (NSDI) with the goal of sharing geographic data through standards, policies, and procedures. Through subcommittees and working groups, the FGDC has several geospatial data standards completed or in some stage of development. These include the Cadastral Data Content Standard, the Spatial Data Transfer Standard, the Spatial Data Accuracy Standard, the Address Content Standard, and the Government Unit Boundary Data Content Standard.

The FGDC has developed the Content Standard for Digital Geospatial Metadata (CSDGM) <http://fgdc.er.usgs.gov/metadata/contstan.html> to be used by all federal agencies. This metadata standard is composed of 334 different elements (119 of which only contain sub-elements). The FGDC also coordinates the National Geospatial Data Clearinghouse for participants worldwide interested in sharing digital geospatial data that conforms to the CSDGM. In the future, the CSDGM is expected to be modified to be made compliant with an emerging international metadata standard, ISO 19115.

Minnesota Department of Administration, Office of Enterprise Technology. *Minnesota Enterprise Technical Architecture.* Version 2.02, 2006.
<http://www.oet.state.mn.us/>

The Minnesota Office of Enterprise Technology (OET) is charged with establishing and maintaining a state information architecture as specified in Minnesota Statue, Chapter 16E.04 Subdivision 2. According to the OET, "This technical architecture is established to describe technology components of the State's information infrastructure and their individual principles, practices and standards that are to be used to guide the development and delivery of all information systems services. The architecture will provide a reference so that various groups of government IT professionals have a consistent view of the information systems infrastructure and the methods that they employ to develop and deliver information systems services." Chapter 4, Data and Records Management, describes the framework for managing information resources, as well as the standards and guidelines that apply.

Minnesota Historical Society, State Archives Department. *Metadata Resources.*
<http://www.mnhs.org/preserve/records/metadata.html>

> *This web site offers annotated links to State Archives and Minnesota projects, as well as to metadata resources particularly relevant to archival and recordkeeping issues.*

State of Utah GILS (Government Information Locator Service) Project. *GILS Resources.* <http://www.utah.org/GILS/resources.htm>

> *Government Information Locator Services (GILS) are in use in a number of states and in agencies of the federal government. They are designed to provide access to the public to government records, library holdings, web sites, and other types of information resources. The State of Utah has compiled a comprehensive and informative list of references and links to GILS conferences, studies, metadata, metadata mapping schemes, and authority list resources.*

UK GovTalk. *Interoperability: Metadata* <http://www.govtalk.gov.uk/interoperability/metadata.asp?order=title>

> *The government of the United Kingdom is developing a comprehensive plan for e-government, which includes standards for interoperability and metadata. This site provides information on, among other things, the UK's Dublin Core-based metadata standard, implementation plans, and a catalog of government functions.*

File Naming

Summary

A file name is the chief identifier for a record. In the world of electronic records, the record's file name provides metadata that places the record in context with other records, records series, and records retention schedules. In most organizations, the policy for naming a file (and hence a record) is left to individuals or to groups of individuals (e.g., departments, committees). Consider establishing an agency-wide file naming policy that complements your electronic records management strategy.

Consistently named records foster collaboration based on mutual understanding of how to name files and use file names (including the file name metadata). Consistently named records also help you to meet your legal requirements. Legally, your records must be trustworthy, complete, accessible, legally admissible in court, and durable for as long as your approved records retention schedules require. Records that are consistently and logically named are easier to manage to meet these requirements.

In other words, with each staff member consistently naming electronic records, another staff member will be able to look at a record's file name and use the information in the record's file name to recognize the contents and characteristics of the record and to make decisions about the record. For example, a staff member could see that "HF0035broch96/97P.pdf" is a brochure about a House bill (HF0035) in the 1996/1997 session that is available to the public.

Legal Framework

For more information on the legal framework you must consider when developing a file naming policy, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook*. Also review the requirements of:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to maintain their accountability and specifies that the medium must enable the records to be permanent. It further stipulates that you can copy a record and that the copy, if trustworthy, will be legally admissible in court.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records using approved records retention schedules.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), mandates that government records should be accessible to the public unless categorized as not-public by the state legislature.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

Key Concepts

As you develop your file naming policy, you will need to be familiar with the following:

- Differences among file names, file paths, and addresses
- Common file name elements
- General challenges in file naming
- Internet file naming protocols
- Domain names
- URL protocols
- Challenges in Internet-based file naming
- General file naming issues

Differences Among File Names, File Paths, and Addresses

A *file name* is the name of the file as it stands alone. The *file path* shows the location of the file. For example, the file "CommitteeAMinutes021401.doc" might be stored in a series of nested directories for all committees as: "X:Committees/CommitteeA/Minutes/2001/February/CommitteeAMinutes021401.doc." An *address* describes the location of a file delivered on the Internet. For example, a map of a public park named Smith Park might have the following address: "http://www.parks.org/smith.html."

Common File Name Elements

When developing your file naming policy, you may wish to include some of the following common elements:

- Version number (e.g., version 1 [v1, vers1])
- Date of creation (e.g., February 24, 2001 [022401, 02_24_01])
- Name of creator (e.g., Rupert B. Smith [RBSmith, RBS])

- Description of content (e.g., media kit [medkit, mk])
- Name of intended audience (e.g., general public [pub])
- Name of group associated with the record (e.g., Committee ABC [CommABC])
- Release date (e.g., released on June 11, 2001 at 8:00 a.m. central time [61101_0800CT])
- Publication date (e.g., published on December 24, 2003 [pub122403])
- Project number (e.g., project number 739 [PN739])
- Department number (e.g., Department 140 [Dept140])
- Records series (e.g., SeriesX)

General Challenges in File Naming

As you develop your policy, you will encounter the following challenges in file naming:

- *Version control*. You will need to determine how and whether to indicate the version of the record. Some organizations put current and obsolete drafts in different electronic file folders without altering the file name. However, when these records are moved from the active electronic file folder to another storage area, identical file names may conflict and cause confusion.
- *Uniqueness*. To avoid file names conflicting when they are moved from one location to another, each record's file name should be unique and independent from its location. For example, if letters are simply named with the word *letter* and the date, they are not independent from location because they could fit into any records series that contains letters, and all letters sent on that date would have the same file name.
- *Persistence over time*. File names should outlast the records creator who originally named the file. With good stakeholder and staff input, and training, you should be able to develop file names that make sense to staff members once the file creators are no longer available.
- *Access and ease of use*. The policy should be simple and straightforward. A simple policy will help staff members logically and easily name records and help ensure that records are accessible to staff members and/or to the public (as determined by the MGDPA). A simple policy will be more consistently used, resulting in records that are consistently named, and thus easier to organize and access.
- *Ease of administration*. The policy should work with your computer infrastructure, so that you can monitor policy compliance, manage records and records series, gather metadata, and perform other administrative tasks easily and in compliance with all legal requirements. For example, if all the records in a specific records series are easily identifiable by file name, they will be easier to gather and manage.

- *Scalability*. Consider how scalable your file naming policy needs to be. For example, if you want to include the project number, don’t limit your project numbers to two digits, or you can only have ninety-nine projects.

Internet File Naming Protocols

Several file naming protocols are currently in use on the Internet. They all fall under the category of Uniform Resource Identifiers (URIs). *URIs* are short text strings that identify resources (e.g., documents, images, electronic mailboxes) on the Internet. These text strings commonly appear in the address window of web browsers. The first part of a URI specifies the *transfer protocol* in use (the method for transmitting the file from one device to another, such as hypertext transfer protocol [HTTP]). The second part specifies the address, often including the domain name, of the file.

Within the broad grouping of URIs are:

- *Uniform Resource Locators (URLs).* URLs are specific schemes that allow browsers and other software to access resources on the Internet. URLs indicate the resource’s location (e.g., address and name).

- *Persistent Uniform Resource Locators (PURLs)*. PURLs are functionally URLs, but act as an intermediary for the URL of a web site by redirecting the browser to a PURL server instead of the actual URL. The PURL server associates the PURL with the real URL and returns the URL to the viewer’s browser.

- *Uniform Resource Names (URNs)*. URNs are designed to serve as persistent, location-independent resource identifiers. Some overlap exists between URLs and URNs, and some URNs are PURLs. URNs are intended to overcome the problem of persistence and location-independence by providing a long-term identifier for resources. URNs use a resolution service to enable a web browser to use the URN to find the URL location for the resource.

Domain Names

Common practice is to include the domain name in the URI. A domain name, such as “microsoft.com,” is nearly always a part of the URL, because URLs identify resources by location. Review the resources in the Annotated List of Resources for more information on domain names. Domain names are administered by the Domain Name System.

URL Protocols

You will encounter several common types of URL transfer protocols, including:

- *Hypertext Transfer Protocol (HTTP)*. This is the most common type of URL protocol accessed on the Internet (e.g., http://www.mnhs.org).

- *File Transfer Protocol (FTP).* This protocol type is commonly used to transfer large files via the Internet (e.g., ftp://ftp.mm.com).

- *Gopher*. This protocol was used primarily in academic and governmental settings, and is rarely used today.

- *News*. This protocol accesses newsgroups (e.g., news:rec:knitting).

- *Telnet*. This protocol allows users to control the activity on another computer and participate in interactive sites for such activities as games, live chats, and text information exchange.

- *Mailto*. This protocol is for e-mail exchange.

Challenges in Internet-Based File Naming

Naming for the Internet is particularly challenging. File names should meet your general criteria, especially for uniqueness, independence from location, and persistence over time. The file names should persist even if you move the files to another server, reorganize your web site, or use another software program or method for producing your web pages.

A carefully constructed policy for naming Internet-delivered files will ensure that:

- *Your web site links stay live*. Links contain embedded information about the location of the resource being linked to. Moving files from one server to another may result in dead links. If you develop a policy that builds in persistence and location-independence, you should be able to avoid this problem.

- *You can more easily manage your web site records*. Because the file names are independent of location, you can be assured that you will be able to find records if they are reorganized. For example, if a department within your agency reorganizes its web pages and moves some files to another server, as long as the file names of the records are independent of location, you can still efficiently manage and archive them.

- *Your Internet-accessed files mesh with your other electronic files*. By integrating your file naming policy with that used for other electronic records, your public records will remain accessible as long as necessary and not-public information will be protected as appropriate.

General File Naming Issues

General issues to consider as you develop a file naming policy include:

- *Determining what metadata to collect*. You will need to decide what metadata to collect and include in file names. Collection and use of metadata in file names will help ensure the long-term usefulness of your records and help you to meet legal requirements for accessibility (for public records) and accountability, as well as protect not-public records.

- *Universal retrieval*. Ensure that the staff and the public (as appropriate) can access your files. Legally, public records must be accessible. Standard file names allow users to find records efficiently.

- *Determining the official copy*. Determine which file is the "official" copy. As part of your web content management (see the *Web Content Management* guidelines), you should include in your policy which web site files are official records, and which version of the electronic file is the official record. Including an indicator of official record status in a file name may be useful for this purpose. The inclusion of this parameter in your policy will help you meet your legal requirements to capture records as set forth by the Official Records Act. The inclusion of this designation may also make administration of your web site records easier.

- *Determining file naming boundaries*. Pay close attention to the freedom you give staff members (and outside vendors) in naming files. Provide guidelines and training on file naming. You will not be able to manage every electronic record's file name, so you will need to rely on staff members and vendors to name files in compliance with your policy. By providing guidelines and training, you can maximize policy compliance in a way that meets your operational and legal requirements.

- *Relationship to and connection with paper records*. Determine how the names of your electronic records relate to the names of paper files you have stored. Because electronic records may be part of records series that include paper records, the file naming policy for electronic records should fit logically with your paper records naming. For example, a letter published on a web site might be part of a records series that includes additional paper documents in a file folder. By ensuring that the electronic records' and the paper records' file names mesh, you can more easily manage the records series.

Key Issues to Consider

Now that you are familiar with some of the basic concepts of file naming, you can use the questions below to discuss how they relate to your agency.

Pay special attention to the questions posed by the legal framework, including the need for public accessibility, as appropriate. Consider your current and future activities and records to help determine the components of a file naming policy that will work now and in the future. For example, you may currently publish official statements or press releases on paper, but in the future, you may publish such records on the web.

Discussion Questions

- Who will use the file naming policy to name files? What policy will make sense to each group?

- Who will need access to these records? Are there different groups with different needs (e.g., the public, internal users)? How will people “think of” this record (e.g., “I need to find a copy of XYZ.doc.” or “I need information about legislation passed in 2002/2003.”)?

- Will the records move location (e.g., from one server to another, from a server to long-term storage)? How will these changes affect file naming?

- What style issues are important? For example, how should the record names appear in print?

- How does file type affect file name? Does our software or computer system limit the number of digits in the file name?

- What types of electronic records will we name?

- How will staff members and the public access and open files in the short-term and long-term? What limitations do these systems have for file naming?

Annotated List of Resources

Primary Resources

Cool URIs Don't Change. In: *Style Guide for Online Hypertext*. Cambridge, MA: World Wide Web Consortium (W3C), 1998.
<http://www.w3.org/Provider/Style/URI>

> *This section of the complete style guide discusses the file naming concepts for the World Wide Web to ensure the accuracy of links and the longevity of the names.*

Naming and Addressing: URIs, URLs,….
<http://www.w3.org/Addressing>

> *These web pages describe the relationship of URIs, URLs, and URNs. The pages also provide links and other information about other file naming topics for the web, such as metadata, markup languages, events, and history.*

Webopedia
<http://webopedia.internet.com>

> *This comprehensive online encyclopedia for the information technology community provides an easy-to-understand, searchable database of terms and topics, including entries on file names and file formats.*

PURL
<http://purl.oclc.org/>

> *The OCLC PURL Service provides a comprehensive introduction to the subject of PURLs. Available from this web site are Frequently Asked Questions on PURLs, introductions to the subject, and the opportunity to create and modify a PURL.*

Additional Resources

Identifiers for Digital Resources. Washington, D.C.: Library of Congress, National Digital Library Program, 1996.
<http://memory.loc.gov/ammem/award/docs/identifiers.html>

> *These web pages describe the desirable characteristics for file naming for digital records. For illustrative purposes, the pages use the American Memory Collection as a case study for a file naming scheme.*

Mims, J. "Files Control." In *Records Management: A Practical Guide*. Washington, D.C.: International City County Management Agency, 1996: 73–84.

> *This chapter on file management discusses such topics as filing systems, filing system creation, filing system maintenance, and filing system equipment. This chapter also offers information on troubleshooting file system control. The content focuses primarily on*

paper systems, but the management principles apply across all media.

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.*

File Formats

Summary

Rapid changes in technology mean that file formats can become obsolete quickly and cause problems for your records management strategy. A long-term view and careful planning can overcome this risk and ensure that you can meet your legal and operational requirements.

Legally, your records must be trustworthy, complete, accessible, legally admissible in court, and durable for as long as your approved records retention schedules require. For example, you can convert a record to another, more durable format (e.g., from a nearly obsolete software program to a text file). That copy, as long as it is created in a trustworthy manner, is legally acceptable.

The software in which a file is created usually has a default format, often indicated by a file name suffix (e.g., *.PDF for portable document format). Most software allows authors to select from a variety of formats when they save a file (e.g., document [DOC], Rich Text Format [RTF], text [TXT] in Microsoft Word). Some software, such as Adobe Acrobat, is designed to convert files from one format to another.

Legal Framework

For more information on the legal framework you must consider when developing a file format policy, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook.* Also review the requirements of:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to maintain their accountability and stipulates that the medium must enable the records to be permanent. It further stipulates that you can copy a record and that the copy, if trustworthy, is legally admissible in court.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records using approved records retention schedules.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that government records should be accessible to the public, unless categorized as not-public by the state legislature.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

Key Concepts

As you consider the file format options available to you, you will need to be familiar with the following concepts:

- Proprietary and non-proprietary file formats
- File format types
- Preservation: conversion and migration
- Compression
- Importance of planning
- File format decisions and electronic records management goals

Proprietary and Non-proprietary File Formats

A file format is usually described as either proprietary or non-proprietary:

- *Proprietary formats*. Proprietary file formats are controlled and supported by just one software developer.
- *Non-proprietary formats*. These formats are supported by more than one developer and can be accessed with different software systems. For example, eXtensible Markup Language (XML) is becoming an increasingly popular non-proprietary format.

File Format Types

Below are brief descriptions of the basic files you are likely to encounter. You can use the resources in the Annotated List of Resources for more detailed information on specific file formats. Basic file format types include:

- *Text files*. Text files are most often created in word processing software programs. Common file formats for text files include:

  - Proprietary formats, such as Microsoft Word files and WordPerfect files, which carry the extension of the software in which they were created.

  - RTF files, which are supported by a variety of applications and saved with formatting instructions (such as page layout).

  - Portable Document Format (PDF) files, which contain an image of the page, including text and graphics. PDF files are widely used for read-only file sharing. However, only Adobe Acrobat can make a PDF file, and Acrobat is necessary for reading a PDF file.

- *Graphics files*. Graphics files store an image (e.g., photograph, drawing) and are divided into two basic types:

  - Vector-based files that store the image as geometric shapes stored as mathematical formulas, which allow the image to be scaled without distortion. Common types of vector-based file formats include:

    - Drawing Interchange Format (DXF) files, which are widely used in computer-aided design software programs, such as those used by engineers and architects

    - Encapsulated PostScript (EPS) files, which are widely used in desktop publishing software programs

    - Computer Graphics Metafile (CGM) files, which are widely used in many image-oriented software programs (e.g., Photoshop) and offer a high degree of durability

  - Raster-based files that store the image as a collection of pixels. Raster graphics are also referred to as bitmapped images. Raster graphics cannot be scaled without distortion. Common types of raster-based file formats include:

    - Bitmap (BMP) files, which are relatively low-quality files used most often in word processing applications

    - Tagged Image File Format (TIFF) files, which are widely usable in many different software programs

    - Graphics Interchange Format (GIF) files, which are widely used for Internet applications

    - Joint Photographic Experts Group (JPEG) files, which are used for full-color or gray-scale images

- *Data files*. Data files are created in database software programs. Data files are divided into fields and tables that contain discrete elements of information. The software builds the relationships between these discrete elements. For example, a customer service database may contain customer name, address, and billing history fields. These fields may be organized into separate tables (e.g., one table for all customer name fields). You may convert data files to a text format, but you will lose the relationships among the fields and tables. For example, if you convert the information in the customer database to text, you may end up with ten pages of names, ten pages of addresses, and a thousand pages of billing information, with no indication of which information is related.

- *Spreadsheet files*. Spreadsheet files store the value of the numbers in their cells, as well as the relationships of those numbers. For example, one cell may contain the formula that sums two other cells. Like data files, spreadsheet files are most often in the proprietary format of the software program in which they were created. Some software programs can import and export data from other sources, including software programs designed for such data sharing (e.g., Data Interchange Format [DIF]). Spreadsheet files can be exported as text files, but the value and relationship of the numbers are lost.

- *Video and audio files*. These files contain moving images (e.g., digitized video, animation) and sound data. They are most often created and viewed in proprietary software programs and stored in proprietary formats. Common files formats in use include QuickTime and Motion Picture Experts Group (MPEG) formats.

- *Markup languages*. Markup languages, also called *markup formats*, contain embedded instructions for displaying or understanding the content of the file. The World Wide Web Consortium (W3C) (http://www.w3c.org) supports these standards. Common markup language file formats include the following:

  - Standard Generalized Markup Language (SGML), a common markup language used in government offices worldwide, is an international standard.

  - Hypertext Markup Language (HTML) is used to display most of the information on the World Wide Web.

  - eXtensible Markup Language (XML) is a relatively simple language based on SGML that is gaining popularity for managing and sharing information.

Table 1 summarizes the common file formats.

Table 1: Common File Formats

File Format Type	Common Formats	Sample Files	Description
Text	PDF, RTF, TXT, proprietary formats based on software (e.g., Microsoft Word)	Letters, reports, memos, e-mail messages saved as text	Created or saved as text (may include graphics)
Vector graphics	DXF, EPS, CGM	Architectural plans, complex illustrations	Store the image as geometric shapes in a mathematical formula for undistorted scaling
Raster graphics	TIFF, BMP, GIF, JPEG	Web page graphics, simple illustrations, photographs	Store the image as a collection of pixels which cannot be scaled without distortion
Data file	Proprietary to software program	Human resources files, mailing lists	Created in database software programs
Spreadsheet file	Proprietary to software program, DIF	Financial analyses, statistical calculations	Store numerical values and calculations
Video and audio files	QuickTime, MPEG	Short video to be shown on a web site, recorded interview to be shared on CD-ROM	Contain moving images and sound
Markup languages	SGML, HTML, XML	Text and graphics to be displayed on a web site	Contain embedded instructions for displaying and understanding the content of a file or multiple files

Preservation: Conversion and Migration

Your most basic decision about file formats will be whether you want to convert and/or migrate your file formats. If you convert your records, you will change their formats, perhaps to a software-independent format. If you migrate your records, you will move them to another platform or storage medium, without changing the file format. However, you may need to convert records in order to migrate them to ensure that they remain accessible. For example, if you migrate records from a Macintosh operating system to a Microsoft Windows operating system, you need to convert the records to a file format that is accessible in the new one (e.g., RTF, Word 2000). For more information on conversion and migration, refer to the *Electronic Records Management Strategy* and *Long-Term Preservation* guidelines.

You will face three basic types of loss determining your course of action:

- *Data*. If you lose data, you lose, to a varying degree, the content of the record. Bear in mind that, legally, your records must be complete and trustworthy.

- *Appearance*. You also risk loss of the structure of the record. For example, if you convert all word processing documents to RTF, you may lose some of the page layout. You must determine if this loss affects the completeness of the record. If the structure is essential to understanding the record, this loss may be unacceptable.

- *Relationships*. Another risk is the loss of the relationships of the data in the file (e.g., spreadsheet cell formulas, database file fields). Again, this loss may affect the legal requirement for complete records.

Keep in mind that a copy of a record is legally admissible only if it is created in a trustworthy manner and is accurate, complete, and durable.

Compression

As part of your strategy, you may choose to compress your files. The pros and cons are summarized in Table 2 below.

Table 2: Pros and Cons of File Compression

Pros	Cons
• Saves storage space • More quickly and easily transmittable	• May result in data loss • Introduces an additional layer of software dependency (the compression software)

The greatest challenge in compressing files is that you may lose data. Compression options vary in their degree of data loss. Some are intentionally "lossy," such as the JPEG format, which relies on the human eye to fill in the missing detail. Others are designed to be "lossless." You may choose to compress some files and not others.

Importance of Planning

The challenges of preservation can be overcome with good planning. Use the resources in the Annotated List of Resources, and thoroughly discuss the issues raised in the Key Issues to Consider section, to weigh the specific pros and cons of each option for your agency. Review the decision tree in the *Guidelines on Best Practices for Electronic Information* white paper for preliminary planning and use the workbook in *Risk Management of Digital Information: A File Format Investigation* to assess your unique situation and risk.

File Format Decisions and Electronic Records Management Goals

The goals of electronic records management that may be affected by file format decisions include:

- *Accessibility*. The file format must enable staff members and the public (as appropriate under the MGDPA) to find and view the record. In other words, you cannot convert the record to a format that is highly compressed and easy to store, but inaccessible.

- *Longevity*. Developers should support the file format long-term. If the file format will not be supported long-term, you risk having records that are not durable, because the software to read or modify the file may be not be available.

- *Accuracy*. If you convert your records, the file format you convert to should result in records that have an acceptable level of data, appearance, and relationship loss.

- *Completeness*. If you convert your records, the file format you convert to should meet your operational and legal objectives for acceptable degree of data, appearance, and relationship loss.

- *Flexibility*. The file format needs to meet your objectives for sharing and using records. For example, you may need to frequently share copies of the records with another agency, use the records in your daily work, or convert and/or migrate the records later. If the file format can only be read by specialized hardware and/or software, your ability to share, use, and manipulate the records is limited.

Key Issues to Consider

Now that you are familiar with some of the basic concepts of file naming, you can use the questions below to discuss how those concepts relate to your agency. Pay special attention to the questions posed by the legal framework, including the need for public accessibility as appropriate, completeness, trustworthiness, durability, and legal admissibility. Consider the degree of acceptable data, appearance, and relationship loss. Take a long-term approach so that your file formats will meet your operational and legal requirements now and in the future.

Discussion Questions

- What are our goals for electronic records management?
- How is our agency affected by the legal requirements?
- What current file formats do we use? Will the developer support these formats long-term?
- Are we planning on converting and/or migrating our records?
- What levels of data, appearance, and relationship loss are acceptable?
- What resources do we have for processing and maintaining records?
- How will our decisions affect other groups that may need current and future access to our records (e.g., other government agencies, the public)?

Annotated List of Resources

Primary Resources

Clausen, Lars R. *Handling File Formats*. Denmark: The State and University Library, The Royal Library, May 2004.
<http://www.netarchive.dk/publikationer/FileFormats-2004.pdf>

> *This report is a publication of the Netarchive.dk project, which seeks strategies for archiving the Danish part of the World Wide Web. The report offers a succinct and intelligent analysis of the issues surrounding file format preservation, including the categorization of formats, aspects of preservation quality, assessment criteria for future usability, and preservation strategies.*

DLM Forum. *Guidelines on Best Practices for Using Electronic Information.* Luxembourg: European Communities, 1997.
<http://dlmforum.typepad.com/>
<http://dlmforum.typepad.com/gdlines.pdf>

> *This white paper was published by the DLM Forum, an organization of records management experts from the Member States of the European Union and the European Commission. The paper provides a basic overview of the file formats in use worldwide. Topics include the information life cycle; the design, creation, and maintenance of electronic records; short-term and long-term access; and accessing and sharing information.*

Lawrence, G.W., W.R. Kehoe, O.Y. Rieger, et al. *Risk Management of Digital Information: A File Format Investigation*. Washington, D.C.: Council on Library and Information Resources, 2000.
<http://www.clir.org/pubs/abstract/pub93abst.html>

> *This publication provides an overview of file format issues related to records management strategies. The publication also provides a comprehensive workbook for users to help them develop a records management strategy.*

Additional Resources

Electronic Recordkeeping Resources.
<http://www.kshs.org/government/records/electronic/ermlinks.htm>

> *This web site provides a comprehensive list of links to other Internet resources related to electronic records management. The site is managed by Cal Lee, who originally constructed it while employed at the Kansas State Historical Society. Topics include security, preservation, access, and technology infrastructure.*

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.*

PRONOM: The File Format Registry.
<http://www.nationalarchives.gov.uk/pronom/>

> *PRONOM is maintained by the Digital Preservation Department of the UK National Archives. Visitors to the site can search within five areas (File Format, Product, Vendor, Support Period, and Release Date), each of which offer more options. Choosing "File Format," for instance, allows visitors to search just by extension to get a straightforward list of associated software or by compatible products, which returns a list of products, versions, release dates, vendors, read/write capabilities, and invariance. Links on vendor and product lead to a wealth of additional detail. Reports can be easily printed or exported into XML or CSV (Comma Separated Value file) for further use.*

Wotsit's Format: The Programmer's Resource.
<http://www.wotsit.org>

> *This online catalog of file formats is broken down into categories such as "Graphics Files," "Text Files/Documents," and "Spreadsheet/Database." Visitors can browse each section or can use the provided search engine to zero in on their mark. Each format carries a one-line description and a link to further information either online or in a download file.*

World Wide Web Consortium (W3C)
<http://www.w3.org>

> *W3C is a consortium of organizations around the world that develops and promotes common web protocols. The site contains news, specifications, guidelines, software, and tools for web development on a wide variety of topics, including markup languages and transfer protocols.*

Storage Facilities and Procedures

Summary

As an employee of a Minnesota government agency, you are legally required to keep records of your agency's activities so that you are accountable to the citizens of the state. While the law does not require you to keep records permanently, your approved records retention schedule may dictate that you keep them for extended periods of time (e.g., ten years or permanently). For practical reasons, you may want to remove the records that you do not refer to frequently from high-cost office space to a lower-cost storage facility until their disposal date. If you use a storage facility, you will need to consider:

- *The physical storage space*. Storing your electronic records in a space designed for that purpose will help you maintain your electronic records as long as legally and operationally necessary.

- *Access procedures*. Procedures for access and use of the storage facility must detail who may access the facility, check out records, add records, and dispose of records.

Your storage facility and procedures policy should mesh with your overall records management strategy. Address both operational and legal requirements to ensure that you store and handle your electronic records in accordance with Minnesota law, while also meeting your operational needs.

Legal Framework

For more information on the legal framework to consider when developing a storage facility and procedures policy, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook.* Also review the requirements of:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to maintain their accountability and specifies that the medium must enable the records to be permanent. The Official Records Act further stipulates that you can copy a record and that the copy, if trustworthy, will be legally admissible in court.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records using approved records retention schedules. Coordinate your records retention schedules with your storage facility management to help ensure that you store and dispose of records in accordance with the Records Management Act.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that government records should be accessible to the public, unless categorized as not-public by the state legislature. Carefully consider which records are public and which are not-public under the MGDPA. You must be able to provide access to the stored public records, yet prevent unauthorized access to not-public records.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

Key Concepts

As you discuss and develop a plan for storage facilities and procedures, you will need to consider:

- Storage facility requirements

- Storage facility components

Storage Facility Requirements

The desirable qualities of a storage facility for electronic records are:

- *Adequate floor space*. You will need to consider:

  – The current volume of material (both electronic and paper) you need to store

  – The projected volume of material you will need to store in the future

  – Your records retention schedules, to see how much material is stored at a given time

  – The space requirements of different media (see the *Digital Media* guidelines)—especially if you are considering switching storage media (e.g., electronic media generally requires less space than paper media)

- *Security*. Allow only approved people to access the storage facility. You will want to consider, among other things:

  – A controlled entrance (e.g., security code keypad, smart-card swipe)

  – An alarm system that sounds if an unauthorized person attempts to enter the storage facility

- *Convenient location*. Consider how often you will need to access the records in your offline storage facility to help determine how conveniently located your storage facility needs to be.

- *Adjustable lighting*. Your storage facility will need to have adequate lighting available for people using the facility, but should be relatively dark when not in use to help preserve the stored materials. Bright lights can fade printed material.

- *Ventilation*. Good ventilation will help prevent dampness, mold, and pest infiltration.

- *Temperature and humidity control*. Proper temperature and humidity are essential for preserving electronic records on digital media. Temperatures and humidity levels that that are above or below the recommended range can deteriorate electronic and paper records. You should strive for a consistent environment, without sudden or drastic changes in temperature or relative humidity.

  – The temperature should be between 68 ºF +/- 2 ºF.

  – Relative humidity should be 40% +/- 5%.

- *Clean air quality*. The air in the storage facility should be free from pollutants (e.g., chemically strong cleaning solution fumes). Dust can be particularly damaging to digital media.

- *Damage prevention*. Protect your storage facility from:

  – Pest infestation (e.g., mice, cockroaches, silverfish)

  – Fire, smoke, and sprinkler damage

  – Water damage, either from leaky pipes and leaky foundations, or from trapped moisture in walls, floors, and ceilings

  – Damage from magnets, since magnets can damage digital data on electronic storage media, and thereby damage your electronic records

You may also consider using a third-party storage facility that can store, access, and deliver records to you. Be certain that the third-party facility can meet your operational needs and all legal requirements.

Storage Facility Components

Determine your needs, priorities, and budget for the following components of a storage facility:

- *Storage aids*. Appropriate storage aids for the media may include shelving, file cabinets, and storage boxes. You may also need special cleaning supplies (e.g., lint-free dusting cloths, cotton gloves for handling sensitive media).

- *Facility map*. You will need a map of the storage facility so that you know which records are stored in each area.

- *Circulation control*. Develop a circulation log or other method for tracking facility access and records circulation. For a reliable circulation control system, you will need to develop an indexing system that accounts for all the records stored in the facility. A central authority should manage the index's content. Media options include a paper list, card file, or database. You should be able to look at the circulation control index and determine the exact status of each record (e.g., if checked out, with whom and when due; if disposed of, when destroyed or disposed of; date of final disposition).

- *Acceptance system*. Develop a process that allows agency members to place records into the facility. Items submitted for storage should have, at minimum, the:

  - Name of the records series
  - Public or not-public designation
  - Record series inclusive dates
  - Unique locator number or identifier
  - Name of the agency and/or department submitting the item
  - Records disposal date

- *Special consideration for vital records*. Your vital records should have the best storage facility you can devise and afford. A third-party vendor may provide your best option for the physical storage of vital records. An off-site storage location is best. Be certain that your facility map shows the location of vital records, so that you can locate them immediately should a disaster occur.

- *On-going maintenance schedule*. Establish an on-going system for maintaining the storage facility, including:

  - Regular cleaning, using chemicals that will not leave harmful residue or fumes
  - Procedures for checking deterioration of physical storage media (e.g., warped compact disks, cracked disks, moldy boxes)
  - Procedures for checking deterioration of electronic content (e.g., unreadable disks, inaccurately read records, missing or scrambled information on records)
  - On-going maintenance program (e.g., reading samples, spinning tapes to tighten them)
  - Regular maintenance of storage facility equipment (e.g., furnaces, air conditioners, dehumidifiers)

- *Reading room*. Establishing a separate reading room near the storage facility could improve security, by allowing you to monitor records use.

- *Disaster recovery plan*. As part of your policy, include a disaster recovery plan that provides a series of detailed actions (including who is responsible for executing each step of the disaster plan) if a disaster should occur at the storage facility. Include the response procedures for multiple types of disasters (e.g., flood, fire, smoke, explosion). The goal of the plan should be to have the facility operational and the greatest number of records recovered in the least amount of time. Train staff members and practice the disaster recovery plan. For more information on disaster recovery, refer to the Disaster Preparedness guidelines <http://www.mnhs.org/preserve/records/disaster.html> on the State Archives' web site.

- *Access and use training*. Provide instruction and training for staff members who will be submitting items for storage, accessing stored records, and checking out records. Established guidelines and training will enable you to provide service, stay organized, and protect your records.

Key Issues to Consider

Now that you are familiar with some of the basic concepts of storage facilities and access procedures, you can use the questions below to discuss how those concepts relate to your agency. Pay special attention to the questions posed by the legal framework, including the need for public accessibility and protection of not-public records as set forth in the MGDPA. Consider your current and future activities and records to help determine your requirements for a storage facility and access procedures. The answers to these questions will guide your development of a storage facility that meets your agency's needs and legal requirements.

Discussion Questions

- What are our goals for a storage facility and access procedures? What priority can we place these goals in? How does this prioritization affect our budget?

- Are there other government agencies to share resources with?

- How long do we need to retain our records under the Records Management Act?

- Will we be storing an increasing volume of electronic records and fewer paper records?

- How frequently will the records need to be accessed? How strictly must access to the records be monitored? Will the public access our records directly, or will we access records on behalf of the public? How will we protect not-public records as defined under the MGDPA?

- What are our needs for floor space, storage aids, location, and security systems?

- Will the storage area be maintained in our daily work space or in a separate location? What are the cost differences of our options?

- Are we considering a third-party storage facility? How will we be sure that the third-party can meet all of our legal and operational requirements?

- Who is responsible for enforcing the storage system policy and procedures? Who will maintain the map and index?

- How will we accept and process records into the storage facility?

Annotated List of Resources

Primary Resources

Beyers, Fred R. *Information Technology: Care and Handling for the Preservation of CDs and DVDs – A Guide for Librarians and Archivists*. NIST Special Publication 500-252. Gaithersburg, MD: National Institute of Standards and Technology; Washington, D.C.: Council on Library and Information Resources. October 2003. <http://www.foray.com/images/pdfs/CDandDVDCareandHandlingGuide.pdf>

> *This guide discusses the physical characteristics of various optical media, as well as methods for their proper care and handling to ensure longest possible use in any given environment. A useful glossary is included.*

COOL, Conservation OnLine
<http://palimpsest.stanford.edu>

> *A compilation of materials from other sources about electronic conservation, this web site includes links to resources on disaster recovery, electronic media, electronic formats, and storage environments.*

Minnesota Historical Society, State Archives Department. *Preserving and Disposing of Government Records.* St. Paul: Minnesota Historical Society, May 2008. <http://www.mnhs.org/preserve/records/docs_pdfs/PandD_may2008.pdf>

> *Developed for Minnesota government agencies, this overview of the basic principles of records management includes chapters on defining a government record, taking inventory of your records, developing records retention schedules, preserving archival records, disposing of records, and setting up a records storage area. A list of resources for more information is included, as well as information about applicable state law regarding electronic records management. Originally published by the Minnesota Department of Administration in July 2000, the guide was updated jointly by the Minnesota Historical Society and the Minnesota Government Records and Information Network (MNGRIN) in 2008.*

Additional Resources

Disaster Preparedness. St. Paul: State Archives Department, Minnesota Historical Society, 2000. <http://www.mnhs.org/preserve/records/disaster.html>

> *Also available as a downloadable file, the information on these web pages summarizes the basic concepts of disaster preparedness, including disaster prevention, disaster planning, disaster recovery, and disaster preparedness resources.*

Electronic Recordkeeping Resources
<http://www.kshs.org/government/records/electronic/ermlinks.htm>

This web site provides a comprehensive list of links to other Internet resources related to electronic records management. The site is managed by Cal Lee, who originally constructed it while employed at the Kansas State Historical Society. Topics include security, preservation, access, and technology infrastructure.

Ellis, J., S. McCausland, S. McKemmish, et al., eds. *Keeping Archives*. 2nd ed. Melbourne, Australia: Thorpe in association with the Australian Society of Archivists Inc., 1993.

This book provides chapters that focus on the different aspects of planning and managing archives for all media, including paper and electronic formats. Special topics of interest to the electronic records archivist include special formats (e.g., moving images, sound recordings), and using computers and document imaging systems.

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.

National Archives and Records Administration (NARA)
<http://www.archives.gov/index.html>

For technical guidance on archival preservation and management, visit the web site of the National Archives and Records Administration.

The PC Technology Guide
<http://www.pctechguide.com/storage.htm>

This site is a comprehensive resource on all aspects of the personal computer. Topics include hardware, software, computer use, and digital media.

Digital Media

Summary

On-going and rapid advances in technology dictate that you store your electronic records on media that enable you to meet your long-term operational and legal requirements. Legally, your records must be trustworthy, complete, accessible, legally admissible in court, and durable for as long as you need them. Because every digital storage option will eventually become obsolete, consider digital storage options that will enable you to maintain records by migrating and/or converting them during their required retention period.

Legal Framework

For more information on the legal framework you must consider when selecting digital storage media, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook.* Also review the requirements of:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to fulfill the obligations of accountability and specifies that the medium must enable the records to be permanent. It further stipulates that you can copy a record and that the copy, if trustworthy, will be legally admissible in court.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records using approved records retention schedules.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that government records should be accessible to the public, unless categorized as not-public by the state legislature.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

Key Concepts

Before you determine which digital media will meet your long-term legal and operational needs, familiarize yourself with the following key concepts:

- Digital data
- Sequential versus random access
- Storage measurement
- Media life expectancy
- Magnetic media
- Optical media
- Performance issues

Digital Data

Your electronic records are digital data that are stored on digital media. Digital data exists, at its most basic level, as just 0 and 1, or on and off. For example, black and white photographs in the newspaper are printed as a series of either black or white dots (0 or 1, on or off). The complex organization of a large number of dots allows the human eye to complete the image. The digital data in an electronic record uses the same principle to organize digital data into the record to make the record readable. A bit (short for binary digit) is the smallest unit of data in a computer. A bit has a single binary value, either 0 or 1.

Digital data is stored on digital media. Digital media are divided into two types:

- *Magnetic*. On magnetic media, the digital data is encoded as microscopic magnetized needles on the surface of the medium (e.g., disk or tape).

- *Optical*. On optical media, the digital data is encoded by creating microscopic holes in the surface of the medium (e.g., disk).

For more information on the storage of digital media to preserve longevity, refer to the *Storage Facilities and Procedures* guidelines.

Sequential Versus Random Access

Access to digital information on digital media is divided into two types:

- *Sequential*. Sequential access requires the user to access specific information by accessing the preceding information on the medium. For example, if you want to view a specific portion of a videotape, you must first fast-forward through the preceding portion of the videotape.

- *Random*. Some digital media allow users to access the stored information from any physical place on the media. For example, when you put a disk into your personal computer's disk drive, you can access any single file stored on the disk without having to first access all the files that precede it.

Storage Measurement

The storage capacity of digital media is measured in bytes, the basic unit of measurement:

- 1,024 bytes make a kilobyte (KB)
- 1,024 KBs make a megabyte (MB)
- 1,024 MGs make a gigabyte (GB)
- 1,024 GBs make a terabyte

For example, a one-page, text-only letter might be 20 KB, a graphics file might be 200 KB, and a fifty-page, desktop-published document with graphics might be 2 MB.

Media Life Expectancy

All storage media have finite life spans which are dependent on a number of factors, including manufacturing quality, age and condition before recording, handling and maintenance, frequency of access, and storage conditions. Studies have indicated that under optimal conditions, the life expectancy of magnetic media ranges from 10 to 20 years for different types, while optical media may last as long as 30 years. However, in real life situations, most media life expectancies are significantly less.

Magnetic Media

Magnetic media include:

- *Magnetic disk*. Magnetic disks include the hard disk found in your computer that stores the programs and files you work with daily. Magnetic disks provide random access. Also included are:
  - *Removable hard disk.* These disks are encased in a plastic housing that allows them to be inserted and removed from a processor. In this way, a single processor can have access to the data on multiple hard drives.
  - *Removable disk*. Removable disks include the relatively small-capacity floppy disks, as well as the larger-capacity peripheral disks, such as the Iomega Zip disks.

  - *Cartridge*. Removable cartridges contain disks encased in a metal or plastic casing for easy insertion and removal.

- *Magnetic tape*. Magnetic tapes come in reel-to-reel, as well as cartridge format (encased in a housing for ease of use). The two main advantages of magnetic tapes are their relatively low cost and their large storage capacities (up to several gigabytes). Magnetic tapes provide sequential access to stored information, which is slower than the random access of magnetic disks. Magnetic tapes are a common choice for long-term storage or the transport of large volumes of information.

- *Digital audio tape (DAT)*. DATs are in a cartridge format a little larger than a credit card. The industry standard for DAT cartridge format is a digital data storage (DDS) cartridge. DDS cartridges provide sequential access.

- *Videotape*. Videotape provides sequential access to video footage (e.g., feature films).

Optical Media

Optical media options include:

- *Compact Disk (CD)*. Compact disks come in a variety of formats. These formats include CD-ROMs that are read-only, CD-Rs that you can write to once and are then read-only, and CD-RWs that you can write to in multiple sessions.

- *Write-Once, Read-Many (WORM) disk*. WORM disks require a specific WORM disk drive to enable the user to write or read the disk. WORM disks function the same as CD-R disks.

- *Erasable optical (EO) disk*. The user can write to, read from, and erase from EO disks as often as they can magnetic disks. EO disks require special hardware.

- *Digital versatile disk (DVD)*. These disks are also called digital video disks, but do not necessarily include video. DVD disks are new types of optical disks with more storage capacity than CD-ROMs. Common types of DVDs include:

  - *DVD video*. These DVDs provide a format for showing full-length films using a special DVD player connected to a television set. DVD videos contain a scrambling system that prevents users from copying the contents.

  - *DVD-ROM*. These DVDs are read-only disks that also have enough storage capacity for a full-length feature film. They are accessed using a special DVD drive attached to a personal computer. Most of these drives are backward-compatible with CD-ROMs and can play DVD video disks.

  - *DVD-RAM*. These DVDs are rewritable disks with exceptional storage capacity. They come in one- or two-sided formats.

- *DVD+RW*. DVD+RW is a direct competitor to DVD-RAM with similar functionality and slightly greater storage capacity.

Note: DVD-RAM and DVD+RW are not compatible. The two technologies are being developed by competing vendors and require different hardware.

- *Optical cards.* Optical cards, also known as “smart cards,” are the size of a credit card. They come in read-only and read-write formats. They are not in widespread use except for limited applications, such as automatic teller machines, personal identification for security systems, and airline reservations.

- *Optical tape*. Optical tape is tape coated with optical recording material. Optical tape is not widely used.

Performance Issues

As you discuss your digital media options, consider each option’s performance characteristics in terms of your records management needs.

- *Speed of access*. Consider how quickly you or authorized members of the public may need to access your records. You may find that some types of records require fast access, while others do not. For example, you may need fast access to key policy decisions, but not to employee records.

- *Capacity*. The volume of records that you can store on the medium will be a key consideration. Examine the volume of the records you now store, and try to determine what your needs may be in the future. Consider the official definition of a record and whether that definition will affect the records volume that you need to manage. For example, you may anticipate greater use of e-mail and the expansion of your web site, which would affect the capacity that you need.

- *Longevity*. Research how long the industry will support various media options and compare those figures with the time period that you need to keep your records according to the approved records retention schedule. You may find a medium that meets all your needs, but is not widely used or has a high risk of becoming obsolete, thereby limiting its usefulness in the future.

- *Durability*. Research how easily a given medium can be damaged or will deteriorate. You may find that a medium that deteriorates after three years will still be a suitable option for records that need to be retained for only one year. Be sure to review your records retention periods.

- *Versatility*. If your records contain multiple file formats (as described in the *File Formats* guidelines), research how many file formats a medium can store. For example, a floppy disk cannot store large graphics files, but a CD or a DVD can store graphics, text, audio files, or video files.

- *Portability.* Determine how portable your stored records should be. Some media, such as DVD-ROMs, are very portable, while hard disks in a computer processor are not. You should also consider whether you will need special devices to read the records. For example, not many organizations are equipped with DVD-ROM players. Consider who will be accessing your records. For example, will the public, the press, or other agencies frequently access your records?

- *Compatibility.* Assess the backward and forward compatibility of the digital media you are considering. For example, DVD-ROM drives are backward-compatible for CD-ROMs, but a CD-ROM drive is not forward-compatible for DVD-ROMs. This discussion will help you to determine how often you may need to upgrade supporting computer systems, migrate records, and/or convert records.

- *Cost.* Assess the costs and benefits of each medium you consider. Be sure to discuss the costs of converting and/or migrating records, as well as the basic costs of the system.

Summary

Table 1 summarizes the capacity of the basic digital media options. Research the specific medium and manufacturer for exact specifications, including cost. Because of rapid technology developments in a highly competitive market, the costs for each option change frequently.

Table 1: Storage Capacity of Digital Media Options

Medium	Capacity (Uncompressed)
Magnetic Media	
Removable hard disk	10 GB
Removable disk	1.44–120 MB
Cartridge	10–30 GB
Magnetic tape	20–180 MB
DAT	24+ GB
Videotape	Up to 8 hours of video
Optical Media	
CD	650-800 MB
WORM (CD-R)	650-800 MB
EO	650-800 MB
DVD	4.7–17 GB

Note: Numbers current as of July 2001.

Key Issues to Consider

Now that you are familiar with some of the basic concepts and options of digital storage media, you can use the questions below to discuss how those concepts relate to your agency.

Pay special attention to the questions posed by the legal framework, including the required records retention periods. Examine your current and future records series. Some records series may require large storage capacities, may need to be retained for a long time, or may be frequently accessed by the public, other agencies, or other groups. Prioritizing your needs in light of the legal requirements will help you narrow your discussion and focus your research.

The point is to determine the best option for your agency that meets your legal and operational needs, not merely to automatically upgrade technology. For example, if you are currently using magnetic tape, you may discover that magnetic tape remains your best choice.

Discussion Questions

- What types of records do we need to store (e.g., graphics, text, database text)? What file formats? How large are our record files?
- Which performance issues are most important in our situation?
- How long do we need to retain the records?
- How often will we need to access the records?
- Will all records or specific records series be frequently accessed by the public or other groups?
- How well do our current media meet our needs? What costs would be incurred for supplies, equipment, and training that would be required if we were to switch to or add a new storage medium?
- Are any of the media we are considering expected to become obsolete in the near future? Will the medium, as well as the necessary hardware and software, still be available from a number of suppliers for as long as we need? Has the developer defined a migration path for improved versions of the medium?

Annotated List of Resources

Primary Resources

Beyers, Fred R. *Information Technology: Care and Handling for the Preservation of CDs and DVDs – A Guide for Librarians and Archivists*. NIST Special Publication 500-252. Gaithersburg, MD: National Institute of Standards and Technology; Washington, D.C.: Council on Library and Information Resources. October 2003.
<http://www.foray.com/images/pdfs/CDandDVDCareandHandlingGuide.pdf>

> *This guide discusses the physical characteristics of various optical media, as well as methods for their proper care and handling to ensure longest possible use in any given environment. A useful glossary is included.*

The PC Technology Guide
<http://www.pctechguide.com/04disks.htm#>

> *This site is a comprehensive resource on all aspects of the personal computer. Topics include hardware, software, computer use, and digital media.*

Webopedia
<http://webopedia.internet.com>

> *This comprehensive online encyclopedia for the information technology community provides an easy-to-understand, searchable database of terms.*

Additional Resources

International Council on Archives, Committee on Electronic Records. *Guide for Managing Electronic Records from an Archival Perspective*. Paris: International Council on Archives, 1997.
<http://www.ica.org/sites/default/files/ICA%20Study%208%20guide_eng_0.pdf>

> *This handbook provides a comprehensive overview of electronic records management from an archival perspective. It provides useful information on key concepts, such as life-cycle management, legal issues, technological issues, and implementation tactics for all readers.*

COOL (Conservation OnLine): Electronic Storage Media
<http://palimpsest.stanford.edu/bytopic/electronic-records/electronic-storage-media>

> *These pages are part of the Conservation OnLine, Resources for Conservation Professionals web site at Stanford University. This web page is a collection of materials from other sources about electronic conservation, including resources on disaster recovery, electronic media, electronic formats, and storage environments.*

Bell, R. and A. Waugh. “VERS Standard for the Management of Electronic Record Formats, Appendix Four: Digital Storage Media.” In *Standard for the Management of Electronic Records*.

Version 1.0. North Melbourne, Australia: State of Victoria, 2000. <http://www.prov.vic.gov.au/vers/standards/pros9907/99-7s4.htm>

An appendix to the State of Victoria (Australia) standard for electronic records management outlines the digital media available for electronic records storage.

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002. <http://www.mnhs.org/preserve/records/tis/tis.html>

This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.

Puglia, S. "Creating Permanent and Durable Information: Physical Media and Storage Standards." *CRM: Cultural Resource Management* 22 (1999): 25–27.

<http://crm.cr.nps.gov/archive/22-2/22-02-10.pdf>

Refer to this web page for a list of references on creating and storing records, including paper records, microfilm, and electronic records.

U.S. General Services Administration. "Applying Technology to Record Systems: A Media Guideline." Information Resources Management Services, KML-93-1-R. (Washington, D.C., 1993).

Published in 1993, this booklet from the federal government provides an overview of digital storage media considerations. Topics include an introduction to concepts and definitions of storage options, physical properties of different media (e.g., paper, microfilm, digital storage, magnetic media, optical media), organization records, capturing and converting records, and cost considerations.

Electronic Document Management Systems

Summary

An electronic document management system (EDMS) is an off-the-shelf software program that serves as an access portal to other applications. The primary function of an EDMS is to manage electronic information within an organization's workflow. Only a few EDMSs include records management capability, so if you choose to use an EDMS, you must be sure that it works within your records management strategy. For example, you must be sure it is able to capture a record and provide access security.

Legal Framework

If you choose to use an EDMS, your selection requires a careful, considered balance between your legal requirements and your technological options. Use of an EDMS is not a panacea for implementing your electronic records management strategy. You should not assume that the requirements for a government agency are built into an EDMS. In fact, the use of an EDMS can lead to records management problems, especially for government agencies with specific legal requirements. The decision to use an EDMS requires significant planning and analysis.

Each vendor's EDMS has different degrees of functionality. In an EDMS designed for the private sector, the functions available may not allow you to meet your legal requirements. For example, an EDMS designed for the private sector may be unable to:

- Manage all the required file formats that constitute government records
- Preserve the record's required metadata
- Ensure trustworthiness
- Provide adequate security of not-public information and records

For example, an EDMS may improve collaboration during document development. However, the EDMS also may create multiple copies of a document and may not provide the access security you need to protect not-public records as defined by the Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>).

Therefore, examine the advantages offered by an EDMS in light of your legal requirements as a government agency. These guidelines will guide you in considering the merits of an EDMS.

Key Concepts

As you discuss the merits of an EDMS for your agency, you will need to be familiar with the following key concepts:

- Document workflow integration
- Basic functions
- Optional functions
- Government standards
- Basic process for selecting an EDMS

Document Workflow Integration

You should look for an EDMS that will help you integrate and automate document management and records management at each point in your agency's records continuum. As discussed in the *Electronic Records Management Strategy* guidelines, records should be managed as part of a continuum, rather than as having discrete stages in a life cycle. The right EDMS may increase the ease of this integrated management.

Consider your agency's document workflow. An EDMS should mirror your workflow and enable you to capture and manage records as part of your daily work (one of the requirements for records to be accepted as evidence under the law).

To learn more about which documents are records, refer to the *Electronic Records Management Strategy* guidelines.

Basic Functions

At a minimum, look for an EDMS that provides:

- *Security control*. This function controls which users have access to which information. Any system that you use must be able to protect not-public records as defined by the MGDPA.
- *Addition, designation, and version control*. The EDMS should allow users to add documents to the system and designate a document as an official government record. It should also automatically assign the correct version designation.
- *Metadata capture and use*. The EDMS should allow you to capture and use the metadata appropriate for your agency.

Optional Functions

You may also want an EDMS that can provide:

- *Records management*. An EDMS may integrate and automate records retention schedules, document status designations, and address other aspects of a unique workflow records continuum. Remember that the inclusion of records management functions is the exception.

- *Storage*. This function will allow you to store documents within the EDMS or to centrally manage your adjunct storage system.

- *Free-text search*. This function allows users to search every word in the entire document or a specified group of documents. Other systems search only metadata.

- *Hypertext links*. Some EDMSs will provide hypertext links from one document to another to facilitate navigating and browsing among related documents.

- *Automatic conversion*. Some EDMSs will automatically convert one file format to another when the file is designated as a record (or at another specific point in the workflow). (For more information on conversion, refer to the *Electronic Records Management Strategy* and *Long-Term Preservation* guidelines.)

- *Compound document management*. Some EDMSs manage compound documents better than others. Compound documents are single documents that contain multiple elements (e.g., text, photographs, video, hypertext links).

With so many developers and systems currently on the market, the list above describes only a few of the optional features that your agency may be interested in.

Government Standards

Government agencies are subject to government regulations and guidelines in the selection of an EDMS. Federal guidelines are set forth in the *Department of Defense 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications*. Bear in mind that even though an EDMS may meet all the Department of Defense guidelines, it may not meet all the requirements for the State of Minnesota. Therefore, you must also consider State of Minnesota legal requirements. You must carefully examine if the EDMS supports:

- Adequate security for the protection of not-public records

- Adequate access to public records

- Ability to capture and manage electronic records (if your EDMS has this function) in a way that meets legal requirements for parameters such as trustworthiness, completeness, accessibility, legal admissibility, and durability

- All electronic formats included in the official definition of a government record

For more information on these rules and statutes, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook*. Also review the requirements of:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to fulfill the obligations of accountability. This statute also stipulates that records should be of a permanent quality. If you are going to use an EDMS for records management, be sure that the EDMS can preserve your records as long as legally required.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records. Consider how you will dispose of the records if you are using the EDMS for records management.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that government records should be accessible to the public, unless categorized as not-public by the state legislature. Any EDMS must be able to protect not-public information and records and provide access to records to authorized members of the public. Even if you do not use the EDMS for records management, you must be certain that the system protects not-public information.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

Basic Process for Selecting an EDMS

The following basic process for selecting, implementing, and managing an EDMS should serve as a baseline for you to develop a more specific process for your agency. The basic process includes:

- *Needs assessment*. The first stage is to work with internal stakeholders and understand your legal obligations to determine your unique needs. If you wish to use the EDMS for records management, be sure that you identify trustworthiness, completeness, accessibility, legal admissibility, and durability as needs (as discussed in the *Electronic Records Management Strategy* guidelines). Be sure to think of not only your immediate needs, but also your long-term requirements.

- *Vendor selection*. You will need to carefully select an EDMS vendor. You may need to issue a request for proposals that sets forth your legal requirements and vendor selection criteria. You may also contact other Minnesota government agencies with similar systems. In short, you will want to gather as much information as you can about potential EDMSs as they are used in government agencies.

- *Implementation plan*. You will need to work with the vendor and internal stakeholders to develop a comprehensive implementation plan. The plan should include a:

  - Technological implementation plan that outlines how and when the system will be installed and tested

  - User implementation plan that includes training and system rollout

- *Deployment*. As detailed in your implementation plan, you will need to install and test the system, and train users.

- *Management*. As you use the system, you will need to continue to manage and refine your use of the system.

Throughout each of these stages, you will need to document the entire process, including needs assessment, implementation, management, and refinement. You will also need to document the system itself, including hardware, software, operational procedures, and security measures. You can refer to the *Trustworthy Information Systems Handbook* for information on documenting such a process.

Key Issues to Consider

You should consider your operational and records management requirements, including the legal framework you operate in as a government agency, as well as your desired product features and agency-specific workflow in order to select an appropriate EDMS.

Use the questions below to consider whether to pursue an EDMS, as well as how to select a vendor. Take a long-term approach in discussing these questions. Consider the types of documents and records you create now and which types you may create in the future. Remember to think of your records as needing to be managed along a continuum, rather than in discrete stages.

Discussion Questions

- What are our needs? What are the needs of all involved stakeholders?

- Do we want to use the EDMS just for workflow management or do we want to use it for records management as well?

- Which records do we want to capture and manage using our EDMS?

- Which formats do we use now and which formats are we likely to use in the future?
- What metadata do we need to include?
- How does the legal framework affect our discussion and decision?
- How do we use records now? How will we use records in the future? What records do we need to share and store?
- How do our records fit into our current workflow? How may we need to modify our workflow to accommodate an EDMS? At which points in our workflow do we need to capture records?
- How will we dispose of records in the EDMS? Will the system enable us to transfer, convert, and/or migrate records easily?
- What are the roles and responsibilities of groups and individuals in terms of electronic records management?
- What features are essential to us in a document management system? What features might be the most useful, but nonessential, elements of a document management system? What is our budget?
- How will we mesh a new system with systems currently in place (e.g., e-mail systems, databases, word processing systems)?

Annotated List of Resources

Primary Resources

Association for Information and Image Management International. *Implementation Guidelines and Standards Associated with Web-based Document Management Technologies*. Silver Spring, Md.: Association for Information and Image Management International, 2002. <http://www.project-consult.net/Files/AIIM+ARP1+2002.pdf>

> *This document contains a set of recommended practices for the implementation of selected web-based document management technologies. The document provides specific recommended activities for each phase of implementing such technologies.*

Document Management Avenue
<http://cgi.parapadakis.plus.com/index.php>

> *This web site provides information and links to white papers, vendors, and related sites. The site also provides news, answers frequently asked questions, and lists events for documentation management professionals.*

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.*

The PC Technology Guide
<http://www.pctechguide.com/storage.htm>

> *This site is a comprehensive resource on all aspects of the personal computer. Topics include hardware, software, computer use, and digital media.*

Additional Resources

AIIM International
<http://www.aiim.org>

> *This web site is published by the Association for Information and Image Management (AIIM). AIIM is an international professional organization for "users and suppliers of the content, document and process management technologies that drive e-business." The site includes information about events, articles, industry studies, and white papers. The web site also includes a products and services vendor directory.*

ARMA International
<http://www.arma.org>

Published by ARMA International, this site focuses on strategic information management issues for records and information managers, information technology professionals, imaging specialists, archivists, librarians, and others. The site includes a buyer's guide and virtual trade show of industry vendors, as well as publications, a bookstore, white papers, industry news, legislative updates, and information on industry standards.

CNET Enterprise, Collaboration and Management, Document Management
<http://www.canada.cnet.com/enterprise/0-9533.html>

This portion of the CNET Enterprise web site provides information on document management software products, including EDMS products. The site also has a research library that allows searches and links to articles, industry news, and white papers. The site also allows you to sign up for newsletters related to topics of interest related to document management. CNET Networks, Inc. is a commercial business that provides information, services, and products to the information technology industry.

Records Management Application Compliance Testing
<http://jitc.fhu.disa.mil/recmgt>

This site lists vendors with EDMS products that have been tested and approved by the federal government. The site provides links to the vendor's web sites. The site also provides access to a number of federal guidelines for records management, including the DOD Standard 5015.2 Design Criteria Standard for Electronic Records Management Software Applications.

Preserving the Electronic Records Stored in an RMA (PERM)
<http://www.sdsc.edu/PERM/>

This web site provides information on the joint project between the State Archives of Michigan and the San Diego Supercomputer Center to develop and test a model for the preservation of electronic records in the State of Michigan's records management application (RMA) environment.

Digital Imaging

Summary

Increasingly businesses and government agencies are looking towards digital imaging to enhance productivity and to provide greater access to certain types of information. Digital imaging offers many advantages, including: improved distribution and publication, increased access, streamlined workflows, and a greatly reduced need for physical storage space. In addition, digital images can be used to create text-searchable files through the application of optical character recognition (OCR) software. Digital images can be made available over the web, allowing government agencies and businesses to provide information to business partners or the general public quickly and efficiently.

While digital imaging is becoming increasingly popular and commonplace, you must remember it is an investment with potentially very high up-front costs. Digital imaging should make financial sense for your business or agency. To assure your digitized records are fully admissible in court, they must be trustworthy, complete, and durable for as long as your approved records retention schedules require.

Legal Framework

Imaging is, by state law, a recognized and legitimate form of record reproduction. To assure that your imaged records are fully admissible and meet all evidentiary standards, you should review the requirements of the:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to fulfill the obligations of accountability and specifies that the medium must enable the records to be permanent. It further stipulates that you can copy a record and that the copy, if trustworthy, will be legally admissible in court.

- Uniform Photographic Copies of Business and Public Records as Evidence Act [Minnesota Statutes, Chapter 600.135] (available at: <http://www.revisor.leg.state.mn.us/stats/600/135.html>), which establishes that an accurate reproduction of a record is as admissible in evidence as the original in any judicial or administrative proceeding. It further stipulates that if an accurate and durable reproduction is made, the original record may be destroyed in the regular course of business unless its preservation is required by law.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the disposition of records using approved records retention schedules.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that government records should be accessible to the public unless categorized as not-public by the state legislature.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

To prove the legal admissibility of your digitized records, you will need to demonstrate the records were created in a trustworthy manner. You should be prepared to demonstrate the reliability of your system and show that it leaves no room for the manipulation of the stored record. For more information refer to the State Archives' *Trustworthy Information System Handbook.*

Key Concepts

Before you determine whether digital imaging will meet your long-term legal and operational needs, acquaint yourself with the following key concepts:

- Imaging terms

- File formats

- Image storage

- Metadata

- Justifying the cost

- Choosing a vendor

- Implementation strategy

Imaging Terms

Digital imaging is a process by which a document or photo is scanned by computer and converted from analog format to a computer-readable digital format. After scanning, the original document or photo is represented by a series of pixels arranged in a two-dimensional matrix called a bitmap or raster image. This image can then be transferred onto a variety of electronic storage media, such as CD-ROM, for storage and use.

For a better understanding of imaging you should be familiar with the following terms:

- Pixel Bit Depth: Defines the number of shades that can actually be represented by the amount of information saved for each pixel. These can range from 1 bit/pixel for binary (fax type) images to 24 bits per pixel or greater in high quality color images. The following are current standard bit depths for image files:

Table 1: Standard pixel bit-depths

Bit-depth	Displays	Recommended for
1-bit or "bi-tonal"	black and white	Typewritten documents
8-bit grayscale	256 shades of gray	Black and white photographs, half-tone illustrations, handwriting
24-bit color	Approximately 16 million colors	Color graphics and text, color photographs, art, drawings, maps

Information taken from: *Technical Recommendations for Digital Imaging Projects* (Columbia University Libraries, April 1997), pages 4-5 (available at: http://www.columbia.edu/acis/dl/imagespec.html).

- Resolution: The quality of a digital image is dependent on the initial scanning resolution. Resolution is expressed in the number of dots, or pixels, used to represent an image, expressed commonly as "dpi," dots per inch. You may also see "ppi" (pixels per inch) and "lpi" (lines per inch) used. As the dpi value increases, image quality increases but so does the file size.

  Unlike paper documents, the resolution of photographs is sometimes expressed in the number of pixels across the long-dimension of an image. When creating standard-sized images from photographs or negatives of differing sizes (e.g., 35mm, 4"x 5"), the scanning resolution in dpi varies. In such cases, it is often easier to measure resolution as the number of pixels across an image's long dimension. For example, each of the following files measures 3000 pixels in the long-dimension, although they have varying values of dpi.

Table 2: Resolution as the number of pixels across the long-dimension of an image

Original photo size	Digital image size	Scanning resolution
8”x10”	2400 x 3000 pixels	300dpi
4”x5”	2400 x 3000 pixels	600dpi
35mm negative	2400 x 3000 pixels	2100dpi

Information taken from: Maxine K. Sitts, *Handbook for Digital Projects: A Management Tool for Preservation and Access* (Andover, Massachusetts: Northeast Document Conservation Center, 2000), page 86 (available at: http://www.nedcc.org/oldnedccsite/digital/dman2.pdf).

To determine the scanning resolution you need, you first have to determine the desired quality of your images and the storage capacity of your computer system. You will also need to consider the desired speed of delivery of the images, especially if they will be accessed over the Internet. You may want to scan high-resolution masters of your images and then create lower resolution copies for web delivery. General recommendations for master files are as follows:

Table 3: Recommended scanning resolutions for master files

Material	Recommended resolution (8-bit grayscale and 24-bit color)
Prints, paintings, drawings, textual records	600 dpi
Maps and oversize	600 dpi (300 dpi minimum)
Photographs, negatives, slides	3000-6000 pixels in long dimension, or 600dpi.

Information taken from: *CDL Guidelines for Digital Images* (California Digital Library, April 2008) (available at: http://www.cdlib.org/inside/diglib/guidelines/bpgimages/reqs.html#guidelinesmaster).

- Compression: Data compression saves file space. There are two types of compression, lossless and lossy. Under lossless compression no data is lost (although the file is still compressed). Under lossy compression data is lost. Lossy compression attempts to eliminate redundant or unnecessary information. Depending upon the degree of compression, this information loss may be unnoticeable to the human eye. For example, it is possible for a JPEG file (a lossy compression) and a TIFF file (lossless) to appear exactly the same, although the JPEG file is missing data, making it significantly smaller. These file formats, and others, are discussed in the following section.

File Formats

In any digital imaging project, choosing the file formats you will use is important. Like scanning resolution, the file format directly affects the quality and file size of your images. Choosing the best file format for your needs requires knowing how your images will be used (e.g., archival or display functions), the type of materials you will be imaging (e.g., text, art, graphics, photos), and the desired speed of delivery and the necessary quality of your images.

For many digital imaging projects it is necessary to create master images. Master images are especially necessary when creating a digital archive. They will serve as archival copies and be the basis from which derivative images are subsequently created. For this reason, high quality is crucial; master images must be in a high resolution and lossless format, insuring that the original document is captured as completely as possible. Master images are high quality images, and they facilitate such functions as implementing OCR, verifying textual information, or zooming into details in maps or photographs. The TIFF file format, which allows high resolution and utilizes lossless compression, is well suited for making master images.

Master images, in formats such as TIFF, have large file sizes, making their delivery cumbersome for some web and document management system applications. To enhance the speed of delivery, you can create copy images from the master images. Copy images have smaller file sizes, are of lower quality, and typically use a lossy compression. The JPEG file format is commonly used for copy images.

Common types of digital image file formats include:

- *Tagged Image File Format* (TIFF) files, which are widely usable in many different software programs. TIFF files utilize lossless compression and are commonly used for master copies. TIFF graphics can be any resolution, and they can be black and white, grayscale, or color. TIFF is a very extensible format, allowing variations to be created for specific applications. Variations include *GeoTIFF*, used in cartographic and GIS (geographic information system) applications; *TIFF Class F*, used in faxing applications; and *TIFF/IT*, used in the graphic arts industry. Files in TIFF format end with a .tif extension.

- *Graphics Interchange Format* (GIF) files. GIF supports color and grayscale. Limited to 256 colors, GIFs are more effective for images such as logos and graphics rather than color photos or art. It should be noted that although the GIF format is widely used, it is technically proprietary. A lossless compression, files in GIF format end with a .gif extension.

- *Joint Photographic Experts Group* (JPEG) files. JPEG is a lossy compression technique for color and grayscale images. Depending upon the degree of compression, the loss of detail may be visible to the human eye. Files in JPEG format end with a .jpg extension.

- *Bitmap* (BMP) files. BMP files are relatively low quality and used most often in word processing applications. BMP format creates a lossless compression. Files end with a .bmp extension.

- *Portable Network Graphics* (PNG) files. A lossless compression designed to replace GIF files, PNG files can be ten to thirty percent more compressed than GIFs. PNG is completely patent and license free and is of higher quality than GIF. Files in PNG format end with a .png extension.

- *Portable Document Format* (PDF) files. PDFs are useful for viewing and printing multiple documents and images. Commonly used to capture, distribute, and store electronic documents, PDF preserves the fonts, images, graphics, and overall "look" of the original digital files. As with the GIF format, the PDF format is proprietary, although widely used. Files in PDF often end with a .pdf extension.

For a more in-depth discussion of file formats, refer to the *File Formats* guidelines.

Image Storage

Digital images are stored on digital media. Digital media are divided into two types: magnetic and optical. Examples of magnetic media include:

- *Magnetic disk*. Magnetic disks include the hard disk found in your computer that stores the programs and files you work with daily. Magnetic disks provide random access. Also included are removable hard disks, floppy disks, zip disks, and removable cartridges.

- *Magnetic tape*. Magnetic tapes come in reel-to-reel as well as cartridge format (encased in a housing for ease of use). The two main advantages of magnetic tapes are their relatively low cost and their large storage capacities (up to several gigabytes). Magnetic tapes provide sequential access to stored information, which is slower than the random access of magnetic disks. Magnetic tapes are a common choice for long-term storage or the transport of large volumes of information.

- *Digital Audio Tape (DAT)*. DATs are in a cartridge format a little larger than a credit card. The industry standard for DAT cartridge format is a digital data storage (DDS) cartridge. DDS cartridges provide sequential access.

Optical media options include:

- *Compact Disk (CD)*. Compact disks come in a variety of formats. These formats include CD-ROMs that are read-only, CD-Rs that you can write to once and are then read-only, and CD-RWs that you can write to in multiple sessions.

- *Write-Once, Read-Many (WORM) disk*. WORM disks require a specific WORM disk drive to enable the user to write or read the disk. WORM disks function the same as CD-R disks.

- *Erasable Optical (EO) disk*. The user can write to, read from, and erase from EO disks as often as they can magnetic disks. EO disks require special hardware.

- *Digital Versatile Disk (DVD)*. These disks are also called digital video disks, but do not necessarily include video. DVD disks are new types of optical disks with more storage capacity than CD-ROMs. Common types of DVDs include:

  - *DVD-ROM*. These DVDs are read-only disks that also have enough storage capacity for a full-length feature film. They are accessed using a special DVD drive attached to a personal computer. Most of these drives are backward-compatible with CD-ROMs and can play DVD video disks. DVD-Rs can be written to once and are then read-only.

  - *DVD-RAM*. These DVDs are rewritable disks with exceptional storage capacity. They come in one- or two-sided formats.

- *DVD+RW*. DVD+RW is a direct competitor to DVD-RAM with similar functionality and slightly greater storage capacity.

Note: DVD-RAM and DVD+RW are not compatible. The two technologies are being developed by competing vendors and require different hardware.

It is highly recommended that you store digital images on WORM, CD-R, or DVD-R disks to assure that the stored records are tamper-proof, allowing the greatest security for the data. Rewritable disks, in contrast, are designed to be re-used, making data integrity uncertain.

Because of limited life expectancy, no digital storage medium is adequate for the long-term, archival preservation of records. The most generous estimate of physical obsolescence is thirty years. Technological obsolescence, though, will probably come within five to ten years. As a result, you should assume the need to migrate all your files to a new storage medium on a regular basis. In the meantime, you will need to protect your stored data with a comprehensive back-up system.

For more information on digital storage media, refer to the *Digital Media* guidelines.

Metadata

Metadata is crucial to any digital imaging project, enabling proper data creation, storage, retrieval, use, modification, and retention of your digitized records. In addition, proper metadata helps document the trustworthiness of your system, assuring the legal admissibility of your digitized records in court.

Metadata can be simply defined as "data about data." More specifically, metadata consists of a standardized structured format and controlled vocabulary which allow for the precise description of record content, location, and value. Metadata often includes items like file type, file name, creator name, date of creation, and the record’s classification under the Minnesota Data Practices Act.

For digital images, metadata is especially important in facilitating retrieval. Unless you plan to use OCR, all of your records will be stored as graphic files. The only way to locate specific information will be through its metadata. Metadata makes it possible to locate, use, and evaluate information through standard search criteria such as subject heading, numerical identifier, or keyword. For this to work effectively, you will have to identify the metadata your employees or patrons use to search for records.

For more information concerning metadata, refer to the *Metadata* guidelines.

Justifying the Cost

Digital imaging should make financial sense for your business or agency. While digital imaging is becoming increasingly popular and commonplace, you must remember it is an investment with potentially very high up-front costs.

Is digital imaging financially right for you? A comprehensive cost-benefit analysis is a necessary step in determining the answer. Costs will include system hardware, system software, application software, long-term system maintenance, staff training, vendor costs, and other expenses. Benefits include higher office productivity, lower storage costs, and the option of using the Web to make digitized information easily accessible. Keep in mind that, because of the rapid pace of technological obsolescence, you will need to make continuing investments in all aspects of an imaging application on a routine and frequent basis.

Choosing a Vendor

Most agencies and businesses do not have the appropriate scanning equipment, software, or staff expertise to execute a large digitizing project. For this reason, vendors have become integral to the world of digital imaging. Quality varies among vendors, so selecting the right one is crucial to your project.

Vendors provide digitizing services, technical advice, and sometimes the long-term maintenance of the resulting electronic files. To better choose your vendor, you should become familiar with digitizing technology and the terms used by the industry. You must also have a clear idea of your project and its goals. Questions such as the following must be addressed:

- How much material will be digitized?
- What type of materials will be digitized? Textual documents? Photographs? Maps?
- Who is the intended audience? Staff members? Researchers? The general public?
- What is the required quality of the digital images? High or low resolution? Black and white or color?
- What is the desired end product? A document management system? A searchable online collection?

As technology products and vendors come and go, you should assume and plan for the possibility of business failure and the inevitability of product obsolescence. The best way to protect yourself is to insist on an open systems architecture, using non-proprietary hardware and software. Non-proprietary means that the chosen hardware and software is not specific to that vendor. If proprietary software is unavoidable, it should be licensed beyond the length of the contract. As there will inevitably be some bugs in the system, a contract should completely spell out the provisions for implementation, service, upgrades, and repair.

Implementation Strategy

To successfully implement a digitizing project in a timely manner, you must create an implementation strategy which manages workflow. A digitizing project incorporates a myriad of tasks, the successful management of which can save time and money. While a vendor may be contracted for the project, you will still need to manage an assortment of activities, including the:

- Selection of materials to be digitized
- Preparation of materials, including sorting files, removing staples and paperclips, weeding out unnecessary materials, and conservation of any deteriorating documents.
- Creation of standardized metadata
- Quality control of source materials and digital images
- Staff training on new hardware and/or software
- Advertising, promotion, and user evaluation
- Long-term maintenance of resulting electronic files

Your implementation strategy may include setting up a pilot project. A pilot project will allow you to test the technology, examine the effectiveness of your digital images in providing and managing information for patrons or employees, and help determine how you can better implement a digital imaging system. A pilot project is especially necessary to study the impact and effectiveness of imaging before undergoing a large digitizing project for a whole department or organization.

Phases are an effective approach to implementing large digitizing projects. Rolling out the system in phases enforces an organized and careful approach to implementation. This allows small errors to be caught and corrected before they snowball into large and costly issues. Phases can be applied in several ways depending upon the structure of your organization and scope of your project. For example, you may want to phase in the system by departments or by function. If your project will be implemented over a lengthy time period, you may want to phase in your system beginning with your organization's highest priorities.

Key Issues to Consider

Now that you are familiar with some of the basic concepts of digital imaging, you can use the questions below to discuss how those concepts relate to your agency. Pay special attention to the questions posed by the legal framework, including the need for public accessibility as appropriate, completeness, trustworthiness, and legal admissibility. Consider the resolution and delivery requirements of your digital images, and choose the file formats and digital storage media that will best fit your needs.

The goal is to determine the best option for your agency that meets your legal and operational needs, not merely to automatically upgrade technology. If you cannot justify the costs of digital imaging, keeping your records in their original form may be the best option.

Discussion Questions

- What are our goals for digital imaging?

- How is our agency affected by the legal requirements?

- What is the desired end product? A document management system? A searchable online collection?

- What type of materials will be digitized? Textual documents? Photographs? Maps?

- What is the required quality of the digital images? High or low resolution? Black and white or color?

- What file formats and digital storage media will best fit our needs?

- What are some strategies for implementing our digital imaging project?

- Can we justify the costs of digital imaging?

Annotated List of Resources

Primary Resources

California Digital Library. *CDL Guidelines for Digital Images.* April 2008.
<http://www.cdlib.org/inside/diglib/guidelines/bpgimages/index.html>

These standards, published by the California Digital Library at the University of California, provide recommendations for image quality, file formats, and storage media for digital image collections.

Columbia University Libraries. *Technical Recommendations for Digital Imaging Projects.* April, 1997.
<http://www.columbia.edu/acis/dl/imagespec.html>

These digital imaging recommendations were prepared by the Image Quality Working Group of ArchivesCom, a joint committee between Columbia University Libraries and AcIS (Academic Information Systems at Columbia University. Provides recommendations for image quality, file formats, and other capture and storage issues.

Sitts, Maxine K. *Handbook for Digital Projects: A Management Tool for Preservation and Access*. Andover, Massachusetts: Northeast Document Conservation Center, 2000.
<http://www.nedcc.org/oldnedccsite/digital/dman2.pdf>

This handbook, published by the Northeast Document Conservation Center, is geared towards librarians, archivists, and other cultural or natural resource managers. Provides a basic technical overview of digital imaging and emphasizes project management, cost justification, vendor relations, and related issues.

Additional Resources

Colorado Digitization Project
<http://www.cdpheritage.org/>

A collaborative effort among Colorado's archives, historical societies, libraries, and museums, the Colorado Digitization Project aims to create a statewide digital library. The website features technical guidelines, digitizing standards, a digital imaging glossary, and links to many additional resources.

Cornell University, Department of Conservation and Preservation. *Moving Theory Into Practice: Digital Imaging Tutorial.*
<http://www.library.cornell.edu/preservation/tutorial/>

Produced by the Digital Imaging and Preservation Policy Research (DIPPR) team at Cornell University's Department of Conservation and Preservation, this web tutorial provides an overview of technical and project management issues regarding digital imaging. The tutorial uses examples of actual digital images to demonstrate variations in image quality.

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mmhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.*

Newcombe, Tod. The Local Government Guide to Imaging Systems: Planning and Implementation. *United States: Public Technology, Inc., 1995.*

> *A publication by Public Technology, Inc. (PTI) and the International City/County Managemnt Association (ICMA), this guide emphasizes planning and implementation issues associated with digital imaging projects. Also addressed are policy and legal issues including records retention, ownership and control of images, and public access.*

Technical Advisory Service for Images (TASI)
<http://www.tasi.ac.uk>

> *This website by Technical Advisory Service for Images (TASI), based at the University of Bristol's Institute for Learning and Research Technology (ILRT), provides information for creating and using digital image archives. The site feature technical and project management advice, and a glossary of digital imaging terms.*

E-mail Management

Summary

E-mail messages are potentially official government records, so you should plan for e-mail as part of your electronic records management strategy. The medium is irrelevant. The content of the message determines whether it is a record or not; the content determines to which records series the message belongs; and the content determines how long the message needs to be retained.

Both statute and case law make clear that government agencies have to include e-mail in an overall records management strategy. Currently, few government agencies manage e-mail as records. Managing e-mail is usually left to personal preference or routine systems back-ups and administrative procedures that treat all e-mail alike. These practices can result in serious legal, operational, and public relations risks.

Legal Framework

For more information on the legal framework you must consider when developing an e-mail records management policy, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook*. Also review the requirements of the:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which:

    - Mandates that government agencies must keep records to fulfill the obligations of accountability and stipulates that the medium must enable the records to be permanent

    - Specifies that you can copy a record and that the copy, if trustworthy, will be legally admissible in court. This means that you can copy your e-mail messages to paper or to text files, as long as the record's content, context, and structure are intact.

    - Does *not* differentiate among media. The *content* of the e-mail message determines whether the message is a record.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records, including e-mail records, using approved records retention schedules.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that government records should be accessible to the public, unless categorized as not-public by the state legislature. Managing access to public versus not-public e-mail records is especially important because e-mail is so easily forwarded, misdirected, and sent to groups of people.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

Additional Legal Considerations

Within the context of these laws, you should also consider:

- *The ramifications of the Armstrong litigation*. In Armstrong v. Executive Office of the President (1 F.3d 1274 [DC Cir 1993]), a federal court found in favor of a group of researchers and nonprofit organizations who wanted to prevent the destruction of e-mail records created during the Reagan administration. The court determined that federal government agency e-mail messages, depending on content, *are* public records and that complete metadata must be captured and retained with the e-mail record. Although a federal decision, this litigation has strongly influenced government agencies at all levels. Other agencies are now paying closer attention to their e-mail records management practices, including the capture of metadata.

- *Legal discovery*. When developing your policy, balance your legal and operational requirements with the risk of being engaged in legal discovery. You must meet all government requirements for managing your e-mail records, but you should also be able to respond to discovery in an affordable, efficient, and practical way. Bear in mind that many courts have upheld discovery requests for e-mail records. For more information on the discovery of electronic records, refer to Appendix E of the *Trustworthy Information Systems Handbook*.

Key Concepts

As you develop your e-mail records management policy, you will need to be familiar with the following key concepts:

- Goals of your process

- E-mail policy components

- Training for staff members

- Recommended process for e-mail policy development

Goals of Your Process

Though your agency will develop unique procedures that meet your specific operational and legal requirements, bear in mind the following goals for an e-mail record. An e-mail record should be:

- *Complete*. E-mail records should completely document the transaction. For example, you cannot save just the text and none of the sender information. Complete e-mail records must include all of the following elements, as applicable:
  - Recipient(s)
  - Sender
  - Subject
  - Text
  - Date sent
  - Time sent
  - Complete attachment(s), which should be included in full (not just indicated by file name), because the attachment is part of the record
  - Group list members, so that if an e-mail record simply lists the group name in the recipient field, the recipients can be identified. For example, the group list "HR" (a group list for all the members of the human resources department) should be documented so that each member of the list is named.
  - Directory of e-mail addresses and the corresponding staff member names (e.g., jado25@myorg.net is Jane Doe), so that an e-mail address listed in an e-mail record can be linked to a person
- *Accurate*. The contents of the e-mail record should accurately reflect the transaction.
- *Accessible*. Some e-mail records must be accessible to the public and some should not be publicly accessible, depending on the content of the record and as determined in the MGDPA. All e-mail records, like other electronic records, should be reasonably accessible for the purposes of legal discovery.
- *Manageable*. The e-mail record should be easy for staff members to manage as part of the daily workflow and records management practices. Because you will rely on staff members to implement and use the e-mail records management policy, procedures should be straightforward.

- *Secure*. The e-mail record should reside in a secure system that controls access, storage, retrieval, alteration, and deletion. This goal is particularly important to control access to not-public e-mail records, as set forth in the MGDPA. E-mail records present unique security concerns, because e-mail messages are:
  - Easily manipulated or deleted in the system
  - Easily captured and read by unintended persons
  - Easily forwarded and misdirected by mistake

E-mail Policy Components

The components of an e-mail retention policy should include:

- *Confidentiality*. Include provisions for maintaining confidentiality of not-public records.

- *Assignment of ownership*. Clearly communicate that both the sender and the receiver should save e-mail records to document transactions and responsibilities completely. For example, if Person A sends an e-mail message to Person B with important information that affects agency policy, the transaction includes not only Person A’s sending of the information, but Person B’s receipt of the information.

- *Process for retention*. Guide staff members in determining which e-mail messages are records. Also, outline a procedure for grouping e-mails into records series, as well as a records retention schedule for each series as mandated in the Records Management Act.

- *Process for managing*. Include procedures for organizing, storing, maintaining, accessing, and disposing of e-mail records. Also, establish a procedure for documenting your e-mail records policy, including the software and hardware in use, specific procedures, training efforts, staff member responsibilities, and records retention schedules.

- *Summary of responsibilities*. Make clear the records management responsibilities of staff members and groups (e.g., departments, project teams, committees) as they engage in their daily work.

Training for Staff Members

Staff members will need to be trained on how to answer legal and operational questions about e-mail. Your training and documentation material should set forth guidelines that staff members can follow to answer such questions in the course of their work. Possible questions include:

- Is this e-mail an official record? Is this e-mail message administrative or personal (e.g., “Thursday staff meeting to start an hour late.” or “Let’s do lunch!”)?
- Does this e-mail message have long-term significance (e.g., “New policy finalized.”)? Does this e-mail message document a transaction or operations function (e.g., a process, a decision, or a discussion)?
- Is this e-mail record public or not-public as set forth by the MGDPA?
- What metadata must I capture when I save this e-mail record?
- Which records series does this e-mail record belong in?
- Should I save the complete e-mail record, including attachments and group list names?
- Could this e-mail message ever be required as evidence in a legal action?

Recommended Process for E-mail Policy Development

Use the following steps to guide you as you develop your e-mail records management policy:

1. Identify and organize key stakeholders in your organization.
2. Draft the policy and process with the input of key stakeholders.
3. Meet with key stakeholders, including individual staff members.
4. Finalize the policy with the input and support of key stakeholders.
5. Implement the policy technically by setting up and testing the procedures.
6. Train the staff members on the new procedures. (Training is especially important because you must rely on staff members to ensure the integrity of the procedures.)
7. Implement the policy for staff members on a planned schedule.

On an on-going basis, from initial development to future policy changes, document the development of your e-mail records management policy, the policy itself, and changes to the policy.

Key Issues to Consider

Now that you are familiar with the operational and legal importance of managing e-mail messages as records, you can use the questions below to begin the development of your e-mail management policy. Discussion of the questions below will help:

- Ensure that you meet your legal and operational requirements
- Gather staff member input, support, and compliance with your e-mail management policy
- Integrate your records management policy with your overall electronic records management strategy
- Ensure that staff members manage e-mail records at the appropriate points in the records continuum, rather than as a single records series with one retention schedule (as explained in the *Electronic Records Management Strategy* guidelines)

Discussion Questions

- How can we ensure staff member compliance and understanding? What process is reasonable to ask staff members to comply with?
- How should we train staff members? How accountable should we make staff members for compliance?
- How should we develop our process?
- Which e-mail messages are records?
- What elements of an e-mail record do we need for a complete understanding of the transaction?
- What is the appropriate records series and records retention schedule for each records series? How should e-mail records be organized for long-term storage and access (e.g., project, department, function)? How will we retrieve and dispose of e-mail on our chosen storage media?
- How should our e-mail retention strategy coordinate with our other records management procedures (e.g., store all project-related e-mail with the other project documentation)? What documentation do we need for our process?
- How should we implement the procedures technically and operationally? How can we plan our implementation so the policy is widely used and accepted, but causes minimal disruption to our daily operation?

Annotated List of Resources

Primary Resources

Ginn, M.L. *Guideline for Managing E-mail*. Prairie Village, KS: ARMA International, 2000.

> *Topics covered in this overview of e-mail management include organizational issues (e.g., legal, operational, governmental), creation and use of e-mail, and management of e-mail as a record (including filing, classification, backup, and disaster recovery).*

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.*

National Electronic Commerce Coordinating Committee. *Managing E-Mail.* December 2002.
<http://digitalarchive.oclc.org/da/ViewObjectMain.jsp?fileid=0000070519:000006287185&reqid=766>

> *This guide tackles the perennial problem of e-mail management in a practical manner, offering model policies for use and retention, as well as a model user manual. While the policies acknowledge that e-mail is a record that should be managed on the basis of its content, the underlying assumption is that most e-mail has only transient value, and three retention periods (immediate destruction, limited retention, and archival retention) are proposed. A guide to implementing the models is also included.*

Additional Resources

Utah State Archives and Records Services: Electronic Records
<http://www.archives.utah.gov/main/index.php?module=Pagesetter&func=viewpub&tid=1&pid=201>

> *Visit this web site for links to the e-mail policies of a number of states in the United States, as well as links to additional web resources for records management.*

Web Content Management

Summary

As the state moves towards e-government and the routine use of technology, more and more government agencies will rely on web sites to serve citizens. In doing so, agencies will have to manage their web content effectively Citizens must be able to find the information they want easily and then be able to determine if it is accurate and current. Information they use for transactions or decision-making will have to be preserved; it cannot be online today and gone tomorrow.

Web content management makes government accountable. Web sites contain records that document government activity and the use of tax dollars, just as any paper record does. Government agencies must therefore manage web content with a carefully developed and implemented policy. Legally, web content must be trustworthy, complete, accessible, legally admissible in court and durable for as long as an approved records retention schedule requires. When agencies manage web content to meet these requirements, they are accountable to Minnesota's citizens.

Legal Framework

For more information on the legal framework you must consider when developing a web content management policy, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook*. Also review the requirements of:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to maintain their accountability. A well-constructed web content management policy can help ensure that your web site records help provide this accountability. This statute also stipulates that the medium must enable the records to be permanent and that you can copy a record and that the copy, if trustworthy, will be legally admissible in court. Therefore, though you may originally publish a record on your web site, if you copy the record and save it separately, the record is still legally admissible.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records using approved records retention schedules. Like other records, your web site records must be maintained according to the established records retention schedule.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that government records should be accessible to the public, unless categorized as not-public by the state legislature. You may request data through the Internet or use the data on an agency intranet that must be protected according to the MGDPA.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

Key Concepts

As you develop your web content management policy, you will need to be familiar with the following concepts:

- Internet, intranets, extranets, and the World Wide Web
- Web site records management
- Legal aspects of web content management
- Involving stakeholders
- Internal communication
- Web content file naming
- Web content management policy components
- Metadata and the Dublin Core set
- TagGen tool for metadata capture
- Web site snapshots

Internet, Intranets, Extranets, and the World Wide Web

The *Internet* is the vast network of computer systems that enables worldwide connectivity among users and computers. The Internet allows you to send e-mail messages around the world, transfer large files outside your agency using file transfer protocol (FTP) sites, telnet to another computer, participate in newsgroups, and view the graphical pages of the World Wide Web.

The Internet links a wide variety of resources. These resources all have implications for use and management. There are resources in different formats (e.g., HTML, PDF) using different protocols for access (e.g., HTTP, FTP, telnet), and different resource indicators for locations (refer to the *File Naming* guidelines). Selecting from these options will have consequences that you need to understand and manage.

The technology that enables the Internet to exist also enables extranets and intranets to exist:

- *Extranet*. An *extranet* is a type of Internet site to which organizations allow only selected external access. For example, a government agency extranet may only allow access by the staff of one other specified agency, or specific government officials.

- *Intranet*. An *intranet* is an internal Internet site that cannot be accessed by anyone outside the organization. For example, a government agency may have an intranet for sharing internal administrative information.

Web Site Records Management

Your web site may contain records defined by the Official Records Act, including public and not-public records as described by the MGDPA. You should manage these records as part of your overall electronic records management strategy. Manage records created for, and published on, web sites at each point in the records continuum, rather than as discrete elements in a set life cycle. Your web content management policy should address web site planning, development, and maintenance with an emphasis on records management. For more information on the records continuum, refer to the *Electronic Records Management Strategy* guidelines.

Legal Aspects of Web Content Management

Consider your legal requirements carefully. (For more information on Minnesota rules and statutes, refer to Appendix D of the *Trustworthy Information Systems* and the *Introduction*.) You will need to consider:

- *Public versus not-public*. Determine which web site records are public and which are not-public as described in the MGDPA. For example, you may gather and store confidential data via a web interface. This data should be protected from access as outlined in the MGDPA.

- *Record or non-record*. The State of Minnesota, as outlined in the Official Records Act, does not differentiate among the media on which records are created or stored. The content of the web file determines whether the file is a record.

Involving Stakeholders

Your web content management policy should include all those who are involved in web site creation, administration, and use. Key groups to include are:

- Content creators and experts
- Web site technical experts
- Web site internal users
- Records management staff

Each group should be familiar with:

- Your policy for web content publication, removal, storage, and disposition
- How the policy affects their daily work practices, including their roles and responsibilities under the policy
- Your agency's electronic records management strategy

Internal Communication

Initial and on-going internal communication will be a crucial aspect of your policy, because:

- Many groups are involved in the creation and administration of a web site.
- Much of a web site's content is interrelated.
- Web site content tends to change frequently.

Consider establishing a formal mechanism to keep stakeholders informed of each other's activities related to the web site. This communication will help ensure the trustworthiness of your web site records, since all stakeholders will know when and why content changes.

Web Content File Naming

Consider establishing a file naming protocol for web pages to help ensure ease of management, usability of the site, and internal communication about contents. For more information about web site file naming, refer to the *File Naming* guidelines.

Web Content Management Policy Components

Consider these ideas as you develop your web content management policy:

- *Determination of records*. As you develop your policy (and on an on-going basis), you will need to analyze the content of your web site to determine which elements are records.

- *Complete records.* When you capture the record, you must be sure that you capture enough information to preserve the appropriate content, context, and structure.

    – *Content*. Factual information in the record that documents government business

    – *Context*. Information that shows how the record is related to the business of the agency and to other records

    – *Structure*. Technical characteristics of the record (e.g., file format, data organization, page layout, hyperlinks, headers, footnotes)

- *Records series and records retention schedules.* As with other records, you should manage records on your web site as records series and develop specific records retention schedules for each records series, as outlined in the Records Management Act.

- *Version control*. Because web sites are updated constantly by different individuals and groups, you should develop a method for designating and controlling versions. This practice will help ensure the trustworthiness of your web site.

Metadata and the Dublin Core Set

As part of ensuring that you capture enough information in a record to demonstrate the record's content, context, and structure, you will need to capture metadata. (For more information, refer to the *Metadata* guidelines). Many Minnesota government agencies have elected to use the Dublin Core Metadata Element Set as a standard (NISO Standard Z39.85; ISO Standard 15836). The Dublin Core was designed to be:

- Manageable

- Searchable

- Extensible

You can read more about the Dublin Core at the Bridges project web site listed in the Annotated List of Resources.

The Dublin Core includes:

- *Title*. The name of the resource given by the creator or publisher.
- *Subject*. The topic of the resource.
- *Description*. A short, text description of the resource’s contents.
- *Creator*. The name of the person who created the resource.
- *Publisher*. The name of the entity that published the resource. Note that the publisher is not the person who posted the resource to the web site, but the entity responsible for the publication of the resource, such as your agency.
- *Contributor*. Someone aside from the creator who made a significant contribution to the resource.
- *Date*. Either the creation date or the publication date. Your agency will need to determine which date to use.
- *Resource type*. The category the resource belongs to, such as committee minutes, press release, or report.
- *Format*. The file format of the resource. For more information on file formats, see the *File Formats* guidelines.
- *Identifier*. A text string or number unique to the resource, such as a URL or other formal name. See the *File Naming* guidelines for more information on naming web site files for longevity and ease of use.
- *Relation*. An element that refers to related resources.
- *Source*. Information about the source from which the current resource is derived (e.g., a report which has been abstracted).
- *Rights management*. A text statement regarding copyright and use permissions.
- *Language*. The language used in the resource (e.g., English, Spanish).
- *Coverage*. Either geographic (e.g., Minnesota) or temporal (e.g., the years 2000–2001).

TagGen Tool for Metadata Capture

TagGen is a software tool that facilitates the creation of standardized metadata. It is available free to Minnesota government agencies. Information on using and acquiring TagGen is on the Bridges web site, as listed in the Annotated List of Resources.

Web Site Snapshots

If you must document your entire web site as a record, consider taking web site snapshots, using a software program to enable you to reconstruct your entire web site. For example, an agency set up a short-term extranet web site for a legislative initiative that included a bulletin board for key people to discuss the initiative. For public records purposes, the agency took web site snapshots in order to reconstruct the site completely as it existed at a given point in time.

Key Issues to Consider

Now that you are familiar with some of the basic concepts of web content management, you can use the questions below to discuss how those concepts relate to your agency.

You will want to discuss:

- Changes to content, organization, or administration
- Transactions completed via the web site
- Communication that takes place via the web site (e.g., bulletin boards, live chats, e-mails posted)
- Development of web site
- Versions and history of web site development

Pay special attention to the questions posed by the legal framework, including the need for public accountability, managing public and not-public records, and following records retention schedules. Put yourself in the citizens' place, and think about how they will use your web site. Take into account your current use of the web and your expectations for future use. For example, you may currently publish a newsletter in paper format, but in the future, you may publish the same newsletter on the web.

Discussion Questions

- What information will citizens seek on our web site? How can we ensure that we make the information easy to find? How can we assure those seeking information of the trustworthiness of the information?

- Which elements of our web site are records?

- Which elements of our web site should we track and store? How long are we legally required to retain our web site records?

- How can we build web content archiving into overall web site management?

- How can we build staff awareness and compliance with web content archiving procedures?

- What will be the archival responsibilities for all staff members involved in web site development and management, especially the webmaster and content developers? Who will *authorize* web site content removal? Who will have the responsibility to accomplish the physical removal and archiving of web site content?

Annotated List of Resources

Primary Resources

Archiving Websites. Canberra, Australia: National Archives of Australia, Commonwealth of Australia, 2000.
<http://www.naa.gov.au/recordkeeping/er/web_records/intro.html>

> *These web pages are the official policy of the National Archives of Australia for web site content management as it relates to records management. However, the pages provide a comprehensive overview for the general reader of the records management aspects of managing and archiving a web site.*

Guidelines for Electronic Records Management on State and Federal Agency Websites. Syracuse, NY: National Historical Publications and Records Commission, 1997.
<http://www.ii.fsu.edu/~cmcclure/guidelines.html>

> *These web pages provide the initial findings of a research project that set out to develop a records management strategy for state and federal agency web sites. The web pages offer a series of assumptions (e.g., what a record is) as well as a discussion of such topics as the relationship of web site records management to other policies, exposure analysis, and guidelines for web site management for state and federal agencies.*

Minnesota Department of Natural Resources. *Bridges: Minnesota's Gateway to Environmental Information*.
<http://bridges.state.mn.us>

> *The Bridges project represented a collaboration between Minnesota's environmental agencies with the goal of providing easy access to their electronic resources such as web pages, PDF documents, databases, and geographic data. Resources were cataloged using the Dublin Core metadata scheme and are located through a simple cross-agency search engine (the Inktomi-powered North Star search at the state's main portal). Although the project was completed in July 2000, the web site still offers a number of resources to visitors, including best practice guidelines for web metadata, information on metadata tools, project reports, as well as links to participating agencies, other regional and federal environmental sites, and the Minnesota Governor's Council on Geographic Information.*

Additional Resources

Kansas Information Technology Advisory Board, Electronic Records Committee and Internet Task Force. *Guidelines for Managing Records on Kansas Government Agency Web Sites*. Version 1.0, January 2004.
<http://da.state.ks.us/itab/documents/ERC_Prop_Web_Guidelines.pdf>

> *The Kansas guidelines are based upon a risk analysis methodology. A summary of web-based resource types and a discussion of preservation strategies accompany a set of agency self-assessment tools.*

McCluskey-Moore, N. “Untangling Web Content Management.” *Intranet Journal*. April 18, 2000.
<http://www.intranetjournal.com/articles/200004/im_04_18_00a.html>

> *This article, published in the online* Intranet Journal*, discusses the development and implementation of a process for managing live web content. The article analyzes the benefits of systematic web content management, describes the desirable characteristics of a web content management strategy, and outlines the process of developing a web content management strategy.*

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.*

Electronic And Digital Signatures

Summary

The advent of e-government and e-services is changing the way we do business. Traditionally, we created records on paper and we authenticated a record by signing it in ink. Today, technology is making both paper and ink irrelevant to many business processes.

This has all sorts of consequences, but, whether in ink or in an electronic format, a signature must fulfill the same functions: it has to authenticate the signer and the document. To use electronic signatures effectively, you need to select the appropriate technological application and make sure they meet these legal obligations. Because signatures are important for their legal and evidentiary value foremost, legal concerns must be the guiding factor in the selection of technologies.

Since different laws affect different agencies and governmental functions, you will need to define your legal needs and connect them to your business processes before deciding which electronic signature application is appropriate for you. In addition, you need to consider your technology architecture, since that application has to work with all the others that create, preserve, and make available your records. As you implement an electronic signature application, you will need to document the key features of the system in order to demonstrate its trustworthy operation and establish its evidentiary value.

Key Concepts

When selecting and implementing an electronic signature technology, keep in mind:

- Legal and technological definitions
- Functions of signatures
- Additional legal considerations
- Electronic signature technologies

Legal and Technological Definitions

There is a problem with the terminology we use. In Minnesota and in most states, there is a clear legal distinction between the definitions of “electronic signature” and “digital signature.” This distinction is not made in other forums, especially among information technology communities, where “electronic” and “digital” are used synonymously and interchangeably. Since signatures are important because of their evidentiary value, there should not be any confusion about a technology you might have to describe before a judge.

In Minnesota, these are the important statutory definitions:

Minnesota Statutes, Chapter 645.44 Subd. 14 (available at: <http://www.revisor.leg.state.mn.us/stats/645/44.html>) contains the basic and traditional definition of a signature:

> The signature of a person, when required by law, (a) must be in the handwriting of the person or, (b) if the person is unable to write, (i) the person's mark or name written by another at the request and in the presence of the person or, (ii) by a rubber stamp facsimile of the person's actual signature, mark, or a signature of the person's name or a mark made by another and adopted for all purposes of signature by the person with a motor disability and affixed in the person's presence.

A reliance on this definition would make it virtually impossible to use technology to deliver services and to meet all legal and evidentiary requirements at the same time. To address this problem, and to provide a standard approach to the use of electronic signatures, Minnesota adopted the Uniform Electronic Transactions Act (UETA) in the 2000 legislative session [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>). UETA defines electronic signatures as:

> An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

This definition is not technology specific, and so does not mandate the adoption of any particular hardware or software application. Any technology, theoretically, that could authenticate the signer and the signed document could generate a legally admissible signature, if the parties could demonstrate the trustworthiness of the process that created and preserved the records in question.

Another approach has emphasized the use of a specific application, public key infrastructure (PKI). The Minnesota Electronic Authentication Act [Minnesota Statutes, Chapter 325K] (available at: <http://www.revisor.leg.state.mn.us/stats/325K>) defines a digital signature uniquely in terms of PKI. A digital signature is:

> A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made.

Digital signatures are a particular type of electronic signature. The advantage a digital signature may offer is that, by providing a unique identifier and linking the signature to the record, it can authenticate both the signer and the signed document. This promises to meet legal requirements for admissibility and trustworthiness. A further advantage is that PKI technology can be adaptable to a wide range of applications and so can work with basic office software.

Functions of Signatures

Signatures serve specific functions. The American Bar Association enumerates these as:

- *Evidence*: A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.

- *Ceremony*: The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent inconsiderate engagements.

- *Approval*: In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect.

- *Efficiency and logistics*: A signature on a written document often imparts a sense of clarity and finality to the transaction, and may lessen the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

An electronic signature will have to fulfill some or all of these functions. You should determine which are pertinent to your business processes before selecting a particular electronic signature technology.

Additional Legal Considerations

Many government agencies and functions have unique and specific legislative mandates. These very often include particular concerns for signatures. A simple search of the online version of the Minnesota Statutes for the keyword “signature” generated hundreds of references. You should thoroughly research the statutes applicable to your agency and functions before making any choices about electronic signature technologies.

For example, a federal law, HIPAA, the Health Insurance Portability and Accountability Act of 1996, is concerned with non-repudiation. Non-repudiation “provides assurance of the origin or delivery of data,” so that the sender cannot deny sending a message and the receiver cannot deny receiving it. This prevents either party from modifying or breaking a legal relationship unilaterally. HIPAA holds that only a digital signature technology can currently provide that assurance.

In addition, there are a number of statutes pertaining to government records which you need to understand because any document signed in the course of an official transaction becomes a government record. The most important are:

- Official Records Act [Minnesota Statutes, Chapter 15.17] (available at: <http://www.revisor.leg.state.mn.us/stats/15/17.html>), which mandates that government agencies must keep records to fulfill the obligations of accountability and specifies that the medium must enable the records to be permanent. It further stipulates that you can copy a record and that the copy will be legally admissible in court.

- Records Management Act [Minnesota Statutes, Chapter 138.17] (available at: <http://www.revisor.leg.state.mn.us/stats/138/17.html>), which establishes the Records Disposition Panel to oversee the orderly disposition of records using approved records retention schedules.

- Minnesota Government Data Practices Act (MGDPA) [Minnesota Statutes, Chapter 13] (available at: <http://www.revisor.leg.state.mn.us/stats/13/>), which mandates that your records should be accessible to the public unless categorized as not-public by the state legislature.

- Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>). Both UETA and E-Sign address the issues of the legal admissibility of electronic records created in a trustworthy manner and the application of the paper-oriented legal system to electronic records.

For more information on the legal framework you must consider when developing an electronic signature technology, refer to the *Introduction* and Appendix D of the *Trustworthy Information Systems Handbook*.

Electronic Signature Technologies

The Uniform Electronic Transactions Act (UETA) [Minnesota Statutes, Chapter 325L] (available at: <http://www.revisor.leg.state.mn.us/stats/325L>) purposely allows for a wide range of signature technologies. It says, "An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable."

An example of this is the "click through" option used on many web sites. To order a product, be it a shareware application, an airline ticket, or a book, a web user has to "click through" a page or form that indicates approval of the vendor's conditions for the sale. The system makes it impossible to transact any business without first establishing that agreement. In this instance, there is no "signature" or anything like it. Instead, the system is designed to make it necessary to move from "A" to "C" *only* through "B," with "B" serving as the equivalent of a signature. Authentication is demonstrated by the documentation of the system and its procedures, not by a signed record of a specific, individual transaction.

UETA implicitly legitimates the use of more familiar technologies, such as faxes and imaging, and more exotic ones, such as iris scans, for electronic signatures. In all cases, the key to demonstrating the trustworthiness of a record and its signature is demonstrating the trustworthiness of the system that creates and manages the record. Having sufficient and appropriate systems documentation is the only way to achieve this.

Digital signatures demand the use of a specific technology, PKI. PKI uses two different keys. One key is kept secret (the private key) and the other key is made publicly available (the public key). The two keys are generated simultaneously and collectively; they are known as a “key pair.” Once a message has been signed using one of the two keys, it can only be verified by the other key. The resulting digital signature is a cryptographic checksum computed as a function of the message and the signer’s private key.

Because the digital signature is generated as a function of the key and a unique message, the signature serves two purposes. It authenticates the signer, since only the individual owner has (in theory, anyway) access to the private key. It also indicates the reliability and integrity of the message, since any alteration to the text would invalidate the signature.

This is not the same as encryption. PKI technology was originally developed for encryption (as in the Pretty Good Privacy applications), but the use of a digital signature does not automatically encode a message. In fact, encryption is not covered in the Minnesota Electronic Authentication Act [Minnesota Statutes, Chapter 325K] (available at: <http://www.revisor.leg.state.mn.us/stats/325K>); that only addresses the use of PKI for digital signatures.

The effective use of PKI for digital signatures relies on some policy and organizational factors. There has to be some way to guarantee and to prove that a specific person actually owns a specific key. And there has to be some way to provide quick and easy access to public keys. Because it is completely impractical for each sender and each recipient of a message to work this out on a case-by-case basis, the use of PKI for digital signatures is dependent on the operation of certificate authorities.

A certificate authority is an independent, trusted third party who issues and manages key pairs. To get a key pair, individuals must prove to a certificate authority that they are who they claim to be. The certificate authority also provides secure access to public keys that allow for the validation and verification of signatures. The Minnesota Electronic Authentication Act [Minnesota Statutes, Chapter 325K] (available at: <http://www.revisor.leg.state.mn.us/stats/325K>) creates a mechanism to license and regulate certificate authorities.

Key Issues to Consider

No electronic signature technology in and of itself is sufficient to meet your legal needs. The evidentiary value of your signed records will ultimately rely on your ability to produce legally admissible documentation of your recordkeeping system. In addition, you will, of course, have to produce the electronic records themselves. Just preserving and providing access to electronic records present some daunting challenges. (For more information, refer to the *Electronic Records Management Strategy* guidelines). Adding electronic signatures to the equation can complicate the situation even further.

Every option available to you has its own advantages and disadvantages. Some issues are constant, though:

- Consider technology obsolescence: hardware and software become quickly outdated, often making it difficult, if not impossible, to preserve and provide access to older electronic records. If you are using two different technologies to create and to sign a record, they might "age" at different rates.

- Plan to document your decisions and transactions: understanding your legal needs and addressing them at the design phase of an application are keys to making this work. Keeping documentation up-to-date is an on-going responsibility, which could be complicated if you are relying on a third party. If you are using digital signatures, for example, you need to make sure that your certificate authority is managing its records and documentation adequately.

- Make sure that your electronic signature technology is interoperable with your and your constituencies' other software applications: requiring complex or expensive solutions is probably not practical. It would be especially difficult to ask citizens to buy and maintain multiple signature technologies.

- Evaluate risks and allocate liabilities: one of the functions of signatures is to provide the evidence of agreement to a transaction. There is no guarantee, either with paper or electronic signatures, that all parties will be one-hundred percent satisfied with the results all the time; litigation will always be with us. Because of that, you should understand the risks any system presents and you should manage the liabilities that result.

- Remember that the human side of the equation is critical: no technology will completely address your legal requirements. For example, despite all its attractive features as a technology, a digital signature is only as reliable as the certificate authority standing behind it.

Overall, selecting the appropriate electronic signature technology means defining the criteria you consider important and then determining if your system and proposed application meet those criteria. The criteria should give priority to legal concerns, since signatures are primarily valuable for evidentiary purposes. But your assessment should include the consideration of other factors, such as technology architectures, costs/benefits, your business practices, and all the policies, hardware, software, controls, and audit procedures that are pertinent.

For a model of and methodology for system development and assessment, refer to the *Trustworthy Information Systems Handbook.* For a specific example of the criteria pertinent to a digital signature application, see the American Bar Association's *PKI Assessment Guidelines* (See the *Annotated List of Resources* at the end of these guidelines).

Discussion Questions

- Why do you want to use electronic signatures? What business functions will the technology support?

- Who will have to use and rely on the electronic signature?

- How long will the signatures and the records to which the electronic signatures are affixed have to be preserved?

- Which state and federal statutes pertain to the functions and transactions that generate your signed records? What case law is there?

- How does the electronic signature technology fit into your overall technology architecture? What’s the total cost of the technology? What’s the cost per transaction?

- What sort of electronic signature technologies do your customers use? Will you have to share these records with any other organizations or agencies? What technologies do they use?

- What methodology will you use for documenting your information systems, policies, and practices?

Annotated List of Resources

Primary Resources

American Bar Association. *Digital Signature Guidelines Tutorial*. Washington, D.C.: American Bar Association, 1996.
<http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>

> *In 1996, the ABA's Section on Science and Technology produced the first legal overview of electronic and digital signatures, as well as related concerns. Although there have been many legal and technological developments in the years since, the site still contains fundamental information on signatures that is of value. The term "tutorial" is slightly misleading; this is basically a short essay, but it is the best introduction to signatures available. It has recently been complemented by the ABA's* PKI Assessment Guideline.

American Bar Association. *PKI Assessment Guidelines*. Washington, D.C.: American Bar Association, 2001.
<http://www.abanet.org/scitech/ec/isc/pag/pag.html>

> *The Information Security Committee of the Electronic Commerce Division of the ABA issued a draft version of its* PKI Assessment Guidelines *(PAG) in 2001. The PAG offers a practical guide for the evaluation and assessment of PKI systems and vendors. This is a very detailed document, almost four hundred pages long. It is available as a PDF file. As noted, it is currently a draft and will be updated in the future.*

Blanchette, Jean-Francoise. "Defining Electronic Authenticity: An Interdisciplinary Journey." Workshop on Interdisciplinary Approaches to Achieving and Analysing System Dependability, Florence, Italy, 29 June 2004.
<http://homepages.cs.ncl.ac.uk/michael.harrison/dsn/blanchettejf_authenticity.pdf>

> *Blanchette's paper provides a succinct overview of digital signature and evidence law in the United States and Europe, along with an examination of the signature lifecycle and the technical preservation problems facing the archivists and the cryptographic community.*

McBride Baker & Coles. *Legislative Analysis Database for E-Commerce and Digital Signatures*. Chicago, IL: McBride Baker & Coles, 2001.
<http://www.mbc.com/ecommerce/legislative.asp>

> *McBride Baker & Coles is Chicago law firm with an interest in information technology and the law. The Legislative Analysis Database for E-Commerce and Digital Signatures is a set of tables that allow for the comparative analysis of practices in different states. These tables systematically list and distinguish enacted digital signature legislation and uniform laws. The firm's e-commerce site provides a variety of other tables for study of pertinent issues around the world.*

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 4, July 2002.
<http://www.mnhs.org/preserve/records/tis/tis.html>

> *This handbook provides an overview for all stakeholders involved in government electronic records management. Topics center around ensuring accountability to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.*

National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *Cryptographic Toolkit: Digital Signatures*. Washington, D.C.: NIST, 2001.
<http://csrc.nist.gov/encryption/tkdigsigs.html>

> *NIST's web site provides access to three Federal Information Processing Standards (FIPS) standards for digital signature algorithms, along with a variety of other resources on cryptography.*

Additional Resources

HIPAAdvisory. *Standards for Security and Electronic Signatures*. Montgomery Village, MD: Phoenix Health Systems, 2001.
<http://www.hipaadvisory.com/regs/securityandelectronicsign/electronicsignature.htm>

> *HIPAA, the Health Insurance Portability and Accountability Act of 1996, has created a small industry of guidelines, consultancies, and web sites devoted to explaining how its mandates can be implemented. This site provides easy access to the rules created by the Department of Health and Human Services for "standards for the security of individual health information and electronic signature use by health plans, health care clearinghouses, and health care providers." Since so many important government functions are related to health care, HIPAA's requirements will probably heavily influence the development of standards and technology architectures for electronic signatures.*

State of Washington. *Electronic Authentication*. Olympia, WA: Office of the Secretary of State, 2001.
<http://www.secstate.wa.gov/ea>

> *Washington's digital signature law was a model for a number of other states, including Minnesota. The Secretary of State oversees the implementation of the law and particularly the regulation of certificate authorities. The web site includes useful information and resources on the workings of the law.*

Glossary

Architecture: An enterprise-wide architecture is a logically consistent set of principles that guide the design and development of an organization's information systems and technology infrastructure.

Backward-compatible: The ability of a software program or piece of hardware to read files in previous versions of the software or hardware.

Bitmap (BMP files): A relatively low quality digital image file format, used most often in word processing applications. BMP format creates a lossless compression. Files end with a .bmp extension.

Bits: The smallest discrete units of digital data. Short for binary digit.

Byte: Eight consecutive bits of digital data.

Checksum: A checksum is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived. If the counts match, then one can assume that the complete transmission was received.

Compact Disk (CD): A type of optical disk storage media, compact disks come in a variety of formats. These formats include CD-ROMs that are read-only, CD-Rs that you can write to once and are then read-only, and CD-RWs that you can write to in multiple sessions.

Compound document: A document with multiple elements (e.g., images, text, animation, hypertext).

Compression: A process, using special software, that reduces the file size of a given electronic file.

Conversion: Changing a record's file format, often to make the record software-independent and in a standard or open format.

Digital Audio Tape (DAT): A type of digital storage media, DATs are in a cartridge format a little larger than a credit card. The industry standard for DAT cartridge format is a digital data storage (DDS) cartridge. DDS cartridges provide sequential access.

Digital data: Data that consists, at its most basic level, of just 0s and 1s.

Digital signature: "A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made" [Minnesota Statutes, section 325K.01].

Digital Versatile Disk (DVD): An optical disk with more storage capacity than CD-ROMs, these disks are also called digital video disks, but do not necessarily include video. Common types of DVDs include: DVD-ROM (read-only), DVD-RAM (rewritable), DVD+RW (competitor to DVD-RAM with similar functionality slightly greater storage capacity).

Digital Versatile Disk--Random Access Memory (DVD-RAM): These DVDs are rewritable disks with exceptional storage capacity.

Digital Versatile Disk--Read Only Memory (DVD-ROM): These DVDs are read-only disks that also have enough storage capacity for a full-length feature film. They are accessed using a special DVD drive attached to a personal computer. Most of these drives are backward-compatible with CD-ROMs and can play DVD video disks. DVD-Rs can be written to once and are then read-only.

Digital Versatile Disk + ReWritable (DVD+RW): DVD+RW is a direct competitor to DVD-RAM with similar functionality and slightly greater storage capacity.

Disposal date: The date on which the records retention period for a given records series expires and the records may be disposed of, either by destruction or transfer to the Minnesota State Archives.

Disposition: Either the destruction of a record or the transfer of the record to the Minnesota State Archives.

Dublin Core metadata set: A widely used set of metadata elements that is easily embedded in a web page.

Erasable Optical (EO) disk: The user can write to, read from, and erase from EO disks as often as they can magnetic disks. EO disks require special hardware.

Electronic document management system (EDMS): A software program and supporting hardware that automate and integrate the records management process.

Electronic mail (e-mail): Electronic correspondence sent from one user to one or more recipients.

Electronic record: "A record created, generated, sent, communicated, received, or stored by electronic means" [Minnesota Statutes, section 325L.02].

Electronic signature: “An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record” [Minnesota Statutes, section 325L.02].

Extranet: A type of Internet site to which organizations allow only selected external access.

File name: The name of the file independent of location.

File path: The location of the file as it is stored in a series of directories.

File transfer protocol (FTP): A type of URL that is commonly used to store and exchange large files.

Forward-compatible: The ability of a software program to create files that can be read by more advanced versions of the software.

Free-text search: A document searching function that searches every word in a document or specified group of documents.

Geographic Information System (GIS): A system of hardware and software used for storage, retrieval, mapping, and analysis of geographic data. A GIS can be as complex as whole systems using dedicated databases and workstations hooked up to a network, or as simple as "off-the-shelf" desktop software. A GIS is able to combine and overlay separate layers of geographic data, making it a valuable tool for organizations needing to map and analyze spatial information.

Gigabyte: 1,024 megabytes of digital data.

Gopher: An early URI protocol used primarily in academic and governmental settings that is rarely used today.

Graphics Interchange Format (GIF): A digital image file format, GIF supports color and grayscale. Limited to 256 colors, GIFs are more effective for images such as logos and graphics rather than color photos or art. It should be noted that although the GIF format is widely used, it is technically proprietary. A lossless compression, files in GIF format end with a .gif extension.

Group list: A list of names and e-mail addresses, organized into a group, that enables the e-mail message sender to enter only the group list name when sending an e-mail message to the group list members.

Hypertext: A special type of database system that allows links among documents.

Hypertext transfer protocol (HTTP): A protocol commonly used to access resources on the Internet.

Information: “Data, text, images, sounds, codes, computer programs, software, databases, or the like” [Minnesota Statutes, section 325L.02].

Internet: The vast network of computer systems that enables worldwide connectivity among users and computers.

Intranet: An internal Internet site that cannot be accessed by anyone outside the organization.

Joint Photographic Experts Group (JPEG): A digital image file format, JPEG is a lossy compression technique for color and grayscale images. Depending upon the degree of compression, the loss of detail may be visible to the human eye. Files in JPEG format end with a .jpg extension.

Kilobyte: 1,204 bytes of digital data.

Lossiness: The degree to which data is lost during file compression.

Lossless compression: Refers to data compression techniques in which no data is lost.

Lossy compression: Refers to data compression techniques in which some amount of data is lost. Lossy compression technologies attempt to eliminate redundant or unnecessary information.

Mailto: This protocol is used for e-mail exchange.

Magnetic disk: A type of digital storage media, magnetic disks include the hard disk found in your computer that stores the programs and files you work with daily. Magnetic disks provide random access. Also included are removable hard disks, floppy disks, zip disks, and removable cartridges.

Magnetic tape: A type of digital storage media, magnetic tapes come in reel-to-reel as well as cartridge format (encased in a housing for ease of use). The two main advantages of magnetic tapes are their relatively low cost and their large storage capacities (up to several gigabytes). Magnetic tapes provide sequential access to stored information, which is slower than the random access of magnetic disks. Magnetic tapes are a common choice for long-term storage or the transport of large volumes of information.

Megabyte: 1,024 kilobytes of digital data.

Metadata: Data about data. Information (e.g., creator name, creation date) that is used to facilitate intellectual control of, and structured access to, other information.

Migration: Moving files to another computer platform that may require changing their formats.

Nearline storage: Storage in a system that is not a direct part of the network in daily use, but that can be accessed through the network.

News: A URI access protocol for newsgroups.

Offline storage: The storage of digital data outside the network in daily use (e.g., on backup tapes) that is only accessible through the offline storage system, not the network.

Online storage: The storage of digital data as fully accessible information on the network in daily use.

Optical Character Recognition (OCR): OCR is the recognition of printed or written text characters by a computer. This involves analysis of the scanned-in image, and then translation of the character image into character codes, such as ASCII. OCR is being applied by libraries, businesses, and government agencies to create text-searchable files for digital collections. OCR is also used to help process checks and credit card slips and sort the mail.

Persistent uniform resource locator (PURL): A type of URI scheme that is functionally a URL, but that redirects the user to a PURL server instead of the URL.

Pixel: A dot of color in a raster-based graphics file.

Pixel Bit-Depth: Defines the number of shades that can actually be represented by the amount of information saved for each pixel. These can range from 1 bit/pixel for binary (fax type) images to 24 bits per pixel or greater in high quality color images.

Portable Document Format (PDF): PDFs are useful for viewing and printing multiple documents and images. Commonly used to capture, distribute, and store electronic documents, PDF preserves the fonts, images, graphics, and overall "look" of the original digital files. As with the GIF format, the PDF format is proprietary, although widely used. Files in PDF often end with a .pdf extension.

Portable Network Graphics (PNG) files: A digital image file format, PNG files are designed to replace GIF files. PNG files can be ten to thirty percent more compressed than GIFs. PNG is completely patent and license free and is of higher quality than GIF. A lossless compression, files in PNG format end with a .png extension.

Raster graphics: A type of graphics file that stores the images as a collection of pixels. Also called bitmapped images.

Record: According to the State of Minnesota, an item that documents an official government transaction or action.

"All cards, correspondence, disks, maps, memoranda, microfilm, papers, photographs, recordings, reports, tapes, writings and other data, information or documentary material, regardless of physical form or characteristics, storage media or condition of use, made or received by an officer or agency of the state and an officer or agency of a county, city, town, school, district, municipal, subdivision or corporation or other public authority or political entity within the state pursuant to state law or in connection with the translation of public business by an officer or agency….The term 'records' excludes data and information that does not become part of an official translation, library and museum material made or acquired and kept solely for reference or exhibit purpose, extra copies of documents kept only for convenience of reference and stock of publications and process documents, and bond, coupons, or other obligations or evidence of indebtedness, the destruction or other disposition of which is governed by other laws" [Minnesota Statutes, section 138.17, subd.1].

"Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form" [Minnesota Statutes, section 325L.02].

Recordkeeping: The act or process of creating, maintaining, and disposing of records. See also *Records management*.

Records continuum: An Australian concept that holds that each person who touches the record should manage the record during its existence, using the stage of the record (e.g., creation, use, long-term storage) as a reference point, not a separate function.

Records management: The planning, controlling, directing, organizing, training, promoting, and other managerial activities related to the creation, maintenance, use, and disposition of records. See also *Recordkeeping*.

Records retention period: The length of time a given records series must be kept, expressed as either a time period (e.g., four years), an event or action (e.g., audit), or a combination (e.g., six months after audit).

Records retention schedule: A plan for the management of records listing types of records and how long they should be kept; the purpose is to provide continuing authority to dispose of or transfer records to the Minnesota State Archives.

Records series: Records arranged according to a filing system or kept together because they relate to a particular subject or function or result from the same activity.

Tagged Image File Format (TIFF): A digital image format, TIFF supports black and white, gray-scaled, and color. TIFF is a non-proprietary format offering the option of lossless compression. TIFF files are usually indicated with the .tif extension.

Telnet: A URI access protocol that provides the user remote control (not just access) to another computer. Most commonly used for interactive, text-based sites.

Terabyte: 1,024 gigabytes of digital data.

Transfer protocol: A series of commands that defines how information is formatted, retrieved, and delivered. Usually used in reference to information transferred over the Internet.

Uniform resource identifier (URI): A short text string that describes an item on the Internet. Also known as the resource's "address."

Uniform resource locator (URL): A type of URI scheme that allows users to access resources on the Internet.

Uniform resource name (URN): A type of URI scheme that is designed to serve as a persistent, location-independent resource identifier.

Vector graphics: A type of graphics file that stores the image as a collection of geometric shapes.

Vital record: A record that is essential to the organization's operation or to the reestablishment of the organization after a disaster.

Web site: A collection of Uniform Resource Indicators (URIs) in the control of one administrative entity. May include different types of URIs (e.g., file transfer protocol sites, telnet sites, as well as World Wide Web sites).

Web site snapshot: The capture of a complete web site as a backup copy using special software.