

Basic Electronic Records Management and Preservation

NAGARA/COSA Annual Meeting

Nashville, TN

July 13, 2011

Mark Myers

Electronic Records Archivist
Public Records Division,
Kentucky Department for Libraries and Archives

E-mail: mark.myers@ky.gov

Phone: (502)564-8300 Ext. 244

What is Electronic Records Retention?

“The act of retaining computer-based records in digital storage media for specified, predetermined periods of time commensurate with their value, with subsequent disposal or permanent preservation as a matter of official organizational policy.”

Stephens and Wallace
Electronic Records Retention

Records Management-Archival Principals

Records Management

- Records Should be Clearly Identified
- Records Go Through “Stages” in their “Life Cycle”
- Records Should be Scheduled for Disposition
- Inactive Records Should be Placed in Low-Cost “Records Center” Storage
- Records Should be Destroyed in the Normal Course of Business

Archival

- Records are Managed at the Aggregate or Group Level
- Records are Appraised for their Evidential and Informational Value
- Arrangement is Based Upon Provenance and Original Order
- Preservation Involves Both Physical Property and Intellectual Content
- Access to Historical Records is Key to the Archival Mission

Records Management Challenges

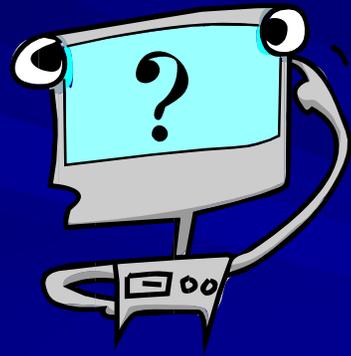
If you're like most governments . . .

- Tradition of under investing in records management
- The whole employee base is affected
- Records are all over the place
- Systems weren't designed for records management
- Tend to operate in functional silos
- Nobody is in charge to the whole program
- The problem's getting bigger every day

Operational Challenges of Electronic Records

- Increasing proliferation of electronic records
- Ease of duplication and dissemination
- Limited control
- Instantaneous change / updates
- Lack of systematic indexing or classification
- Old legacy systems that need to be updated
- Processes are automated without considering recordkeeping needs
- System resources, not records, are managed

What is a Record?



What is Information?

“Communication of knowledge”

Robek, Brown & Stephens,
Information and Records Management, 4th ed

What is Information?

Types of information:

- Static vs Dynamic
- Recurring vs Nonrecurring
- Action vs Nonaction
- Internal vs External

Characteristics of Information:

- Human Readable vs Machine Readable
- Active vs Inactive
- Official vs Nonofficial
- Documentary vs Nondocumentary

What is a Document?

“Recorded Information or object that can be treated (or filed) as a unit.”

- Taken from ISO 15489(1) – Information and Documentation-Records Management

Records as Evidence

Federal Uniform Rules of Evidence, Article VIII, Rule 803 (6) Hearsay exceptions

- Records of **regularly conducted activity**. A memorandum, report, record, or data compilation, **in any form**, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if **kept in the course of a regularly conducted business activity**, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

Records as Evidence

Kentucky Rules of Evidence, Rule 1001 (1)

- Writings and recordings. "Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.

Public (Government) Record

KRS 171.410 defines a public record as:

“all books, papers, maps, photographs, cards, tapes, disks, diskettes, recordings and other documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained by a public agency.”

Public (Government) Record

TCA 10-7-301(6) defines a public record as:

“... all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings, or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency”

National Archives and Records Administration

*“Records. Includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, **regardless of physical form** or characteristics, **made or received** by an agency of the United States Government under Federal law or in connection with the **transaction of public business** and **preserved** or appropriate for preservation by that agency or its legitimate successor as **evidence** of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the **informational value** of data in them. (Source: 36 CFR 1220.14)”*

Business Record

A record created, received, and **maintained as evidence** and information by an organization, in pursuance of **legal obligations** or in the **transaction of business**.

- Taken from **ISO 15489(1) – Information and Documentation-Records Management**

What is an Electronic Record?

Uniform Electronic Transaction Act (UETA) defines electronic record as:

“a record created, generated, sent, communicated, received, or stored by electronic means.”

“Computer Record!”

■ (UETA)

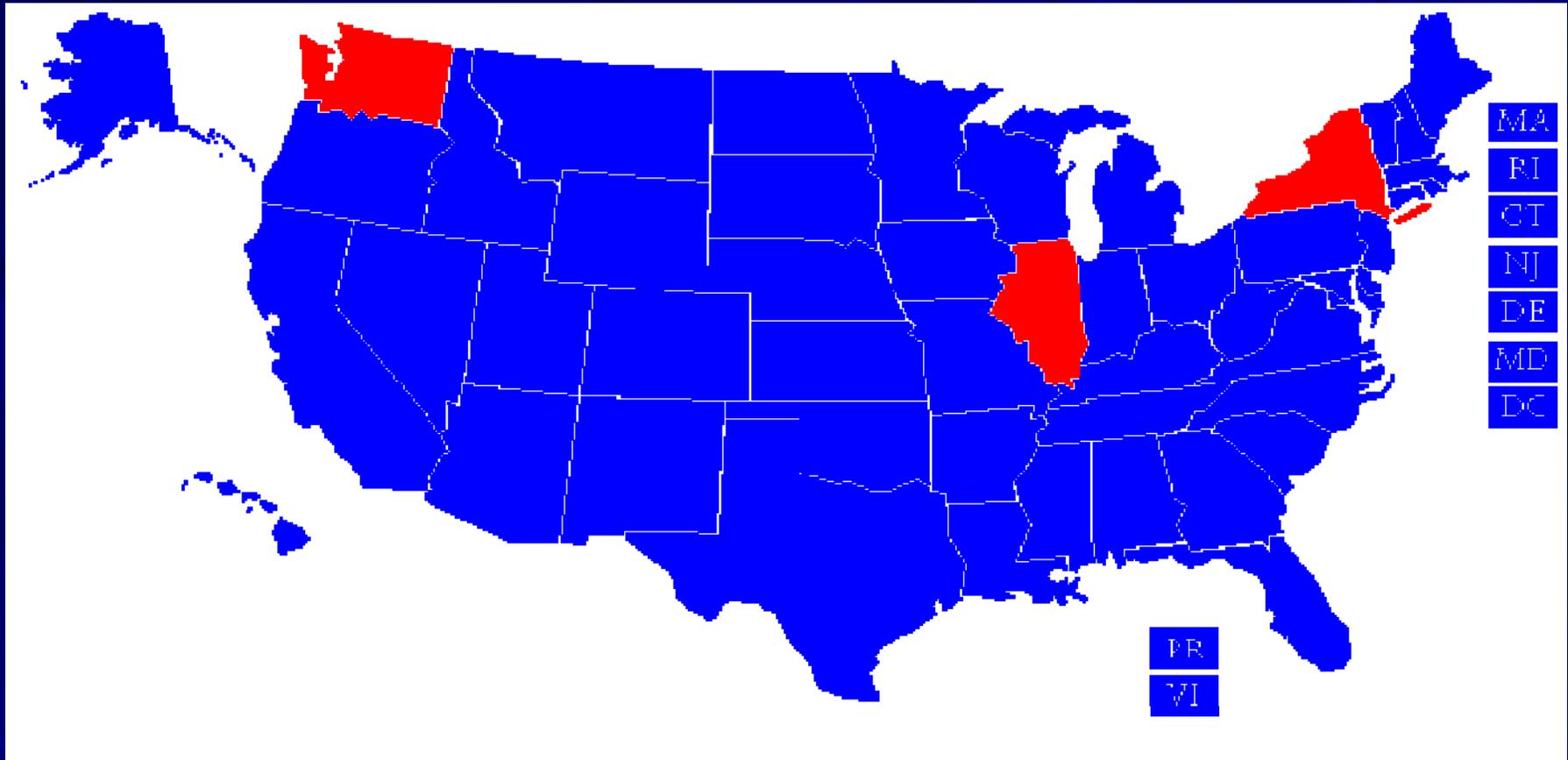
- Model Law passed in 47 states (as of July 2011)
- Follows the federal **E-SIGN Act**
- Validates the use of electronic records, and electronic signatures
- Excludes certain types of transactions – notably Real Property



States and Territories that have enacted UETA

(Source: National Conference of State Legislatures, July, 12, 2011)

<http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/UniformElectronicTransactionsActs/tabid/13484/Default.aspx>



Characteristics of Records?

- **Content** - “Data”
 - What information (data) does the record contain?
- **Structure**
 - appearance and arrangement of the content
- **Context** - “Metadata”
 - Who created the record, when, why and for what purpose?
 - How it relates to other records.

Characteristics of a Record

Regardless of Format

– Paper

– Microform

Eye Readable

– Electronic Records

■ Email

■ Digital Imaging

Machine

Readable

– Audio/Video

– Physical Objects (Artifacts)

Characteristics of Electronic Records

- Born Digital
 - Have always been created electronically,
- Records previously produced in hard copy that are now produced electronically
- Hard copy records that are being reformatted into an electronic form
 - Imaging

Records Life Cycle

- **Birth** - Creation or receipt
- **Working life**
 - Active records – accessed more than 1/month
 - Inactive records – less than 1/month
- **Death** - Ultimate disposition
(destruction or transfer to an archive)



Questions?

Designing an Effective Records Management Program

“Information which is not
communicated is valueless, and
information that cannot be found is
similarly worthless.”

Robek, Brown & Stephens,
Information and Records Management, 4th ed

What is a Records Management Program?

- Records Inventory
- Records Retention Schedule
- Active Records Management
- Electronic Records Management
- Inactive records management
- Records Disposition
 - Record Destruction
 - Archival Record Management
- Vital Records Protection
- Disaster Recovery Planning

Creating a Records Management Program

Step 1: Ensure Accountability and Management

- Obtain management support!!!
- Appoint a records officer
- Form a Records Management Team
 - All major stakeholders: IT, Legal, Fiscal
 - All departmental units
 - Management & Staff

Creating a Records Management Program

Step 2: Assess your Starting Position

- Records Inventory
 - All records – paper, electronic
- Examine existing policies & procedures
- Current capabilities
- Identify high-risk areas
 - Regulations, business operations, litigation

Creating a Records Management Program

Step 3: Records Retention Schedule

- Foundation of the program
- Sets minimum retention periods
- Covers all media
- Clear destruction procedures
- Always being updated

Records Retention Schedule

- Establish Retention Periods
 - Operational/Administrative Value
 - Fiscal Value
 - Legal Value
 - Historic Value
- Balance
 - Legal and Operational use
 - IT and cheap storage

Other Considerations

- Is this a vital record?
- Volume - Annual accumulation
- Access/Reference Rate
- Input and output records
- Date span
- Formats

Creating a Records Management Program

Step 4: Implementation

- Process not an event
- Get a win early
 - Start with paper records
- Protect High-Risk areas
- Ensure compliance
 - Policies & Procedures
 - Training & Education

Why Develop a Records Management Program?

Measure the cost savings from:

Better Access & Control

- Retrieve info quickly and efficiently
- Use the right information technology for the right reasons.
- Retain the records needed as evidence

Managed Retention

- Gets rid of obsolete records.
- Lower storage costs
 - IT & Paper storage
- Store records safely and securely.

Objectives of a Records Management Program

Active Records Management

- Classification and filing system
- Optimal location
- Official file stations
- Optimal storage medium
- Proper access & security controls

Active Records:
Records Accessed at least once a month

Objectives of a Records Management Program

Inactive Records Management

Inactive Records:
Records accessed less than once a month

- Low cost – high volume storage
 - Can be off-site
 - Can be handled by 3rd party
- Slower Access/Retrieval
- Designed for long-term records

Policies & Procedures

Define Policy Scope

- Control Access & Use
 - Access Procedures
 - Appropriate Content
 - Indexing & Naming
 - Security & Passwords
- Retention & Destruction
 - Regulatory & Compliance considerations
 - Implementation
 - How to destroy
 - Approval process

Issues in Managing Electronic Records

What is Electronic Records Retention?

“The act of retaining computer-based records in digital storage media for specified, predetermined periods of time commensurate with their value, with subsequent disposal or permanent preservation as a matter of official organizational policy.”

Stephens and Wallace
Electronic Records Retention

Types of Electronic Records

- Complex structured data
 - Relational database (Oracle)
 - Object oriented database (e.g. MS Access)
- Semi-structured text records
 - Electronic mail database
- Unstructured files
 - Word processing files
 - Text databases (Notes, litigation support)
- Software dependent systems
 - GIS
 - Imaging systems

Characteristics of an Electronic Record

- Four essential characteristics:
 - **Authenticity**-A record must be what it purports to be.
 - **Reliability**-A record must be a full and accurate representation of the transactions, activities, or facts to which it attests.
 - **Integrity**-A record must be complete and unaltered.
 - **Usability**-A record must be able to be located, retrieved, presented, and interpreted.

**Authenticity + Reliability =
TRUST**



Authenticity & Reliability

- “Virtually all determination of authenticity or integrity in the digital environment ultimately **depends on trust**. We verify the source of claims about digital objects or, more generally, claims about sets of digital objects and other claims and, on the basis of that source, **assign a level of belief** or trust to the claims.”

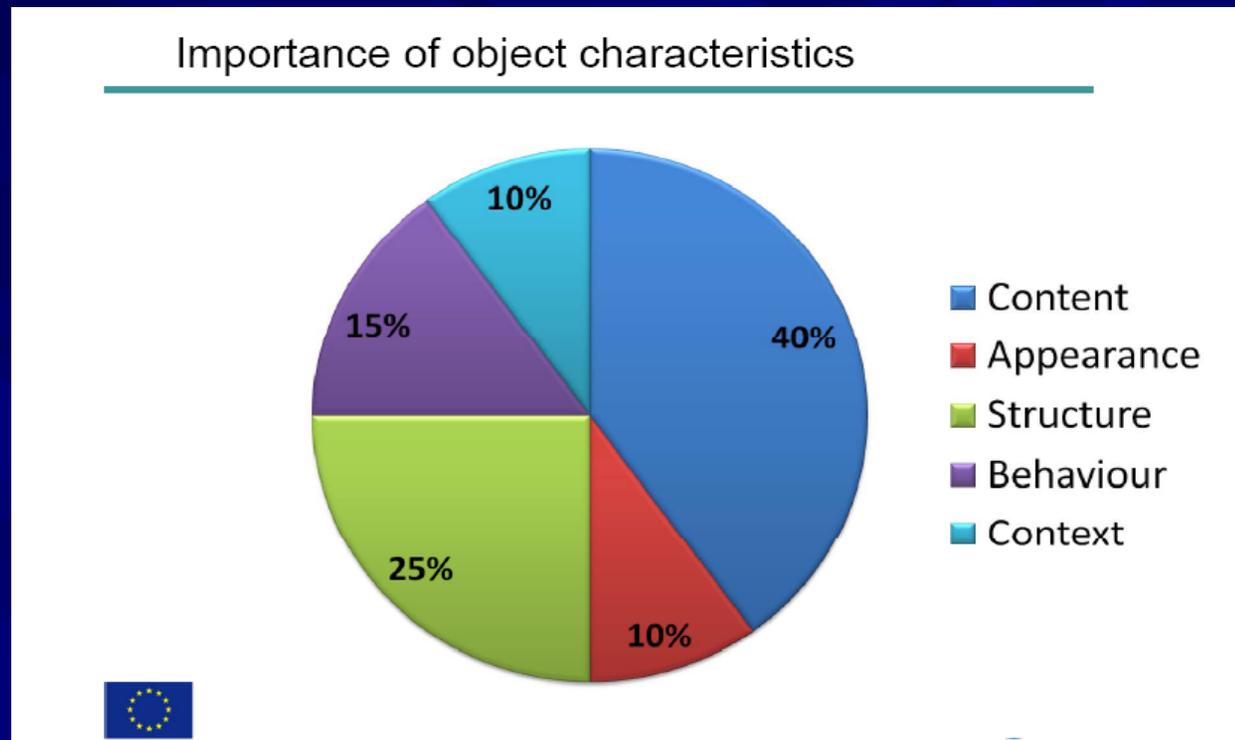
Clifford Lynch, “Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust.” CLIR

Authenticity & Reliability

- “An authentic record is one that can be proven
 - to be what it purports to be,
 - to have been created or sent by the person purported to have created or sent it, and
 - to have been created or sent at the time purported.
- “To ensure the authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment.”

ISO 15489(1) – Information and Documentation-Records Management

European Union: PLANETS



Christoph Becker, et. al. "Preserving Interactive Multimedia Art," 2007 http://www.planets-project.eu/docs/presentations/ICADL_2007_ChristophBecker_Interactiveart.pdf

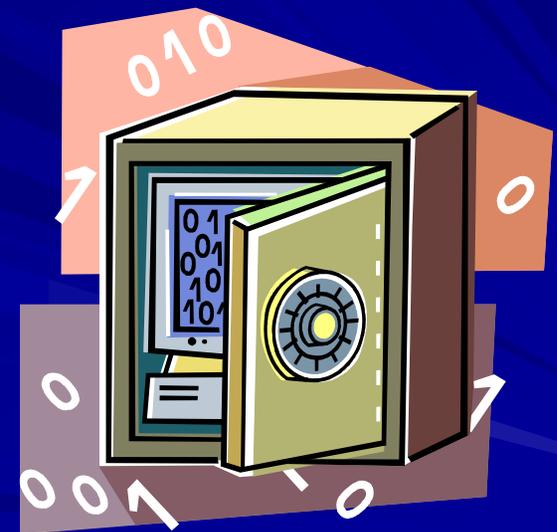
Determining Authenticity

- Since we don't have a stable digital object, we can
 - Document the process used to create it
 - Minnesota's Trustworthy Information Systems
 - Compare it with other known copies
 - LOCKSS
 - Maintain an audit trail of transformations
 - Specify the properties/attributes necessary for authenticity

Integrity: Protecting the records

Must be secure

- Allow for proper access the system
 - Authentication and authorizations
 - Audit Trails
- Protect information
 - Improper access
 - Protect from data loss



Integrity - Data Handling Policies

- Put limits on data collection
 - “Do you really need all of that information?”
- Limit data display and disclosure
 - Don’t print SSN on unnecessary documents
 - Don’t use SSN to link files, as an account number, etc.
- Restrict data access to staff
- Conduct regular staff training
- Social Networking (MySpace/Facebook) presenting new challenges to “privacy”

Integrity - Data Security

- Inventory Data (Records Schedules)
 - Know where your data is
 - Segregate sensitive data from open data
- Avoid the “Bagel Defense”
 - Hard exterior / soft interior
- Think outside the box
 - Laptops, Blackberries/PDAs, mobile computing
- Need policies and guidelines



Integrity – Data Protection

Invest in Protection

■ Firewalls and Network Security

- Make sure software is up to date
 - Regular updates & patches
 - Test before installing on entire network
- Password protect all PC's
 - Train employees in proper use of passwords
 - Require log-ins and registration

■ Install Anti-virus software

- Keep it updated!!

Windows

A fatal exception 0E has occurred at 0028:C00068F8 in UxD UMM(01) + 000059F8. The current application will be terminated.

- * Press any key to terminate the application.
- * Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue

Integrity – Data Security

Back-up

- On a routine basis
 - Daily, Weekly, Monthly
 - Different systems may have different back-up schedules.
- Emergency restoration only – **not for records storage/management**
- Store back-up tapes offsite
- Business/Sensitive data - Use encryption

Usability – Accessing the Record

- For the Entire Life of the Record
- Must design electronic systems with access in mind!
 - Internal – External
 - Formats - Media
 - Restricting Access
 - Incorporate retention requirements

Usability – Accessing the Record

Advantages

- Storage Capacity
- Rapid Retrieval
- Indexing
- Immediate Recording
- Multiple Access points
 - Internal
 - External

Disadvantages

- High Cost
 - Equipment
 - Backfile Conversion
 - Maintenance
 - Migration
- Vendor Responsibility
- Not an Archival Medium

Other Electronic Records Issues: Managing Desktop Records

- Unstructured Records
 - Office applications
- “Personal” versus “Official” records
- Loosely organized
- Often not backed-up
- Need a “Desktop Records Management Policy”

Other Electronic Records Issues: Managing Desktop Records

Desktop Records Management Policy
should cover:

- Purpose/User Responsibilities
- Filing instructions
 - Organization
 - Location
- Retention/Disposition Instructions

Electronic Records Management Tools

International Standard (ISO) 15489-1

- Information and documentation – Records management – Part 1: General

Technical Report ISO/TR 15489-2

- Information and documentation - Records management – Part 2: Guidelines

ISO 15489 Records Management

ISO 15489-1

- Broad principles and requirements of records management

ISO/TR 15489-2

- Methodologies that comply with the standard
- Reference Tables
- Bibliography

Electronic Records Management Tools

■ Electronic Recordkeeping Standards

– DoD 5015.2-STD

- <http://jitc.fhu.disa.mil/recmgt/>
- Criteria for electronic recordkeeping systems for all Defense Department agencies
- Adopted by NARA as a standard for all federal agencies
- Lists all compliant systems and the test criteria
- Version 3 released April 2007

US DOD 5015.2 STD version 3

- (1) **General Information.**
- (2) **Mandatory** – filing, e-mail, storing, scheduling, retrieving, transfer, access & destruction.
- (3) **Management of Classified Records – Optional**
- (4) **Managing Records for the Privacy Act and the Freedom of Information Act**
- (5) **Non-mandatory** – graphical user interface, documentation, hardware environment.

Electronic Records Management Tools

■ Document Management Systems

- Document Repository
- Allows users to create, edit, delete
- Search & Retrieval
- Audit Trails
- Access Controls

■ Electronic Recordkeeping Systems

- Declare a document a record
- Applies Retention Schedule
- Prevents alteration or deletion
- Maintains contextual information
- Access Controls
- Tracks Electronic & Paper Records

Disposing of Data



Why Destroy Records?

- Destroying Records When **Authorized**
 - Keeps Files from getting cluttered
 - Frees up space in the office
- Destroying Records **Systematically**
 - Gives you the legal authority to dispose of records
 - Shows that you have an active records management program in place
- Destroying Records in a **Timely manner**
 - Reduces Legal Liability

Guidelines for Document Destruction

- Destruction periods are determined from the records retention schedule.
- Records eligible for destruction should be carefully reviewed.
 - One copy must be designated as the “record copy” to meet retention requirements.
 - One person should sign-off on destruction

Guidelines for Document Destruction - continued

- Destruction policy should be documented and completed systematically.
 - Keep documentation of destruction
 - Have regular destruction dates
 - End of calendar/fiscal year
 - End of audit
 - Conclusion of projects
- **Employees must be trained on the procedures/policies!**

**“Hitting Delete Doesn’t
Always Mean Delete”**

**Disposing of Electronic
Records**

Disposing of Electronic Records

- Must have policies to control copies
 - Printed and electronic
 - Official or “Record” copy
 - Account for desktops and mobile devices
 - Remember back-up tapes
- Importance of a central file repository
- Simply hitting “Delete” doesn’t remove records



Methods for Deleting Electronic Records

- Common utility programs
 - Relatively cheap and easy to use
- Reformat - “Erase”
- Remove drives
- Physically destroy
 - Only sure way of deleting information
- **Remember back-up tapes!**



SUSPENSION OF DESTRUCTION

DESTRUCTION OF
RECORDS MUST
BE SUSPENDED
IN CASE OF
LITIGATION,
PENDING
LITIGATION, OR
AUDIT



Questions?

Special Topics in Electronic Records

Digital Imaging

Authority to Digitize

- KRS 171.660 allows agencies to:
 - “reproduce and preserve . . . any records or papers by photographic, microphotographic, **nonerasable optical image**, or other process” which:
 - accurately reproduces the original records,
 - forms a durable medium, and
 - which is performed in accordance with rules and regulations promulgated by KDLA

Digital Imaging

Advantages

- Storage Capacity
- Rapid Retrieval
- Indexing
- Immediate Recording
- Multiple Access points
 - Internal
 - External

Disadvantages

- High Cost
 - Equipment
 - Backfile Conversion
 - Maintenance
 - Migration
- Vendor Responsibility
- Not an Archival Medium

Digital Imaging System Planning

Conduct a needs assessment:

- Workflow:
 - Frequency of use
 - Multiple points of access
- Cost/Benefit Analysis
 - Hardware/Software
 - Training
 - Maintenance & Upgrades
- Retention period considerations
 - less than ten years
 - greater than ten years



Digital Imaging System Planning

■ Open Systems Architecture

– Hardware should be **interchangeable**

- not reliant on a single brand or vendor

- Use standard-based system components

– System should be **Scaleable**

- Allows for upgrade and growth with minimal disruption

– Software should be **portable**

- Should work on multiple types of hardware

- Software should allow for **import/export** to other software

Digital Imaging System Planning

■ Image Requirements

- Use non-proprietary, standard image formats
 - Tagged Image File Format (TIFF, .tif)
 - Portable Document Format (PDF, .pdf)
- Scanning Resolution
 - Resolution requirements appropriate for accurate capture of the original
 - 300 dpi (dots per inch) – Black & White Text
 - 600 dpi – Color, drawings, maps, documents with background detail

Digital Imaging System Planning

■ Image Requirements (continued)

– **Compression** – method used to “shrink” image so they occupy less space and can be handled quicker

■ **Lossy** – removes parts of the image the human can't see. Problems occur if resizing the image multiple times.

■ **Lossless** – retains all of the data allowing the image to be resized.

Digital Imaging System Planning

- Image Requirements (continued)
 - Why compress?

| Compression | 200 dpi | 300 dpi | 400 dpi |
|-------------------------------|---------|---------|---------|
| Uncompressed | 500 KB | 1.05 MB | 2 MB |
| Compressed using CCIT Group 4 | 50K | 105 KB | 220 KB |

Digital Imaging System Planning

- Set up appropriate storage environment
 - Should be secure
 - Allow for monitored or controlled access
 - Store images on a central server or hard-drive
 - Could use non-rewritable optical disks (WORM)
 - Do not use removable media
 - CD, DVD
 - Allow for growth and expansion
 - All systems should be backed up on regular schedule with some copies stored off-site.

Digital Imaging System Planning

■ When choosing a Vendor

- Reliable with good track record

 - Local agencies can use the state price-contract list

- Make sure vendors meet your needs – **don't meet theirs**

- Determine Vendor responsibilities

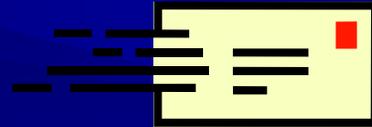
 - Maintenance & Technical Support

 - System Upgrades & Expansion

 - Training

- **You (state/county) maintain control of images**

Issues in E-Mail Management



E-Mail

Some consider email to be the most legally risky form of business communication

- users assume, **incorrectly**, that their messages are private
- email encourages “**chatty**” modes of expression as opposed to more formal, business like communication
- can be **very difficult** to get rid of
- can result in it being a **legal liability**

Anatomy of an Email Message

The screenshot shows an email client window titled "RE: Kentucky City Clerks - Message (HTML)". The message header includes:

- From: Myers, Mark (KDLA)
- To: 'Barbara Combs'
- Cc:
- Subject: RE: Kentucky City Clerks
- Sent: Tue 9/20/2005 10:54 AM

The "Message Options" dialog box is open, showing settings for:

- Message settings: Importance: Normal, Sensitivity: Normal
- Security: Encrypt message contents and attachments, Add digital signature to outgoing message, Request S/MIME receipt for this message
- Tracking options: Request a delivery receipt for this message, Request a read receipt for this message
- Delivery options: Have replies sent to: [empty], Expires after: None, 12:00 AM
- Internet headers: Microsoft Mail Internet Headers Version 2.0
Received: from agsmtp03.eas.ds.ky.gov ([162.114.80.64]) by AGMBX01.eas.ds.ky.gov with Microsoft SMTP5VC(6.0.3790.1830); Mon, 27 Nov 2006 09:57:16 -0500
Received: from ag-east-ex1.kyoag.local ([162.114.238.14]) by agsmtp03.eas.ds.ky.gov with Microsoft SMTP5VC(6.0.3790.1830); Mon, 27 Nov 2006 09:57:15 -0500

The main email body contains the following text:

...or Libraries and Archives. He provides records the management of their electronic records. Prior to ma Department of Archives and History. Mark has a

Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C.Cir., 1993)

...D. Myers (Mark Myers (KDLA)); Mark Morgan; Raymond

RETURN E-MAIL WAS MISDELIVERED WHEN MY NEW COMPUTER

Public Citizen v. Carlin, 184 F.3d 900 (D.C.Cir., 1999)

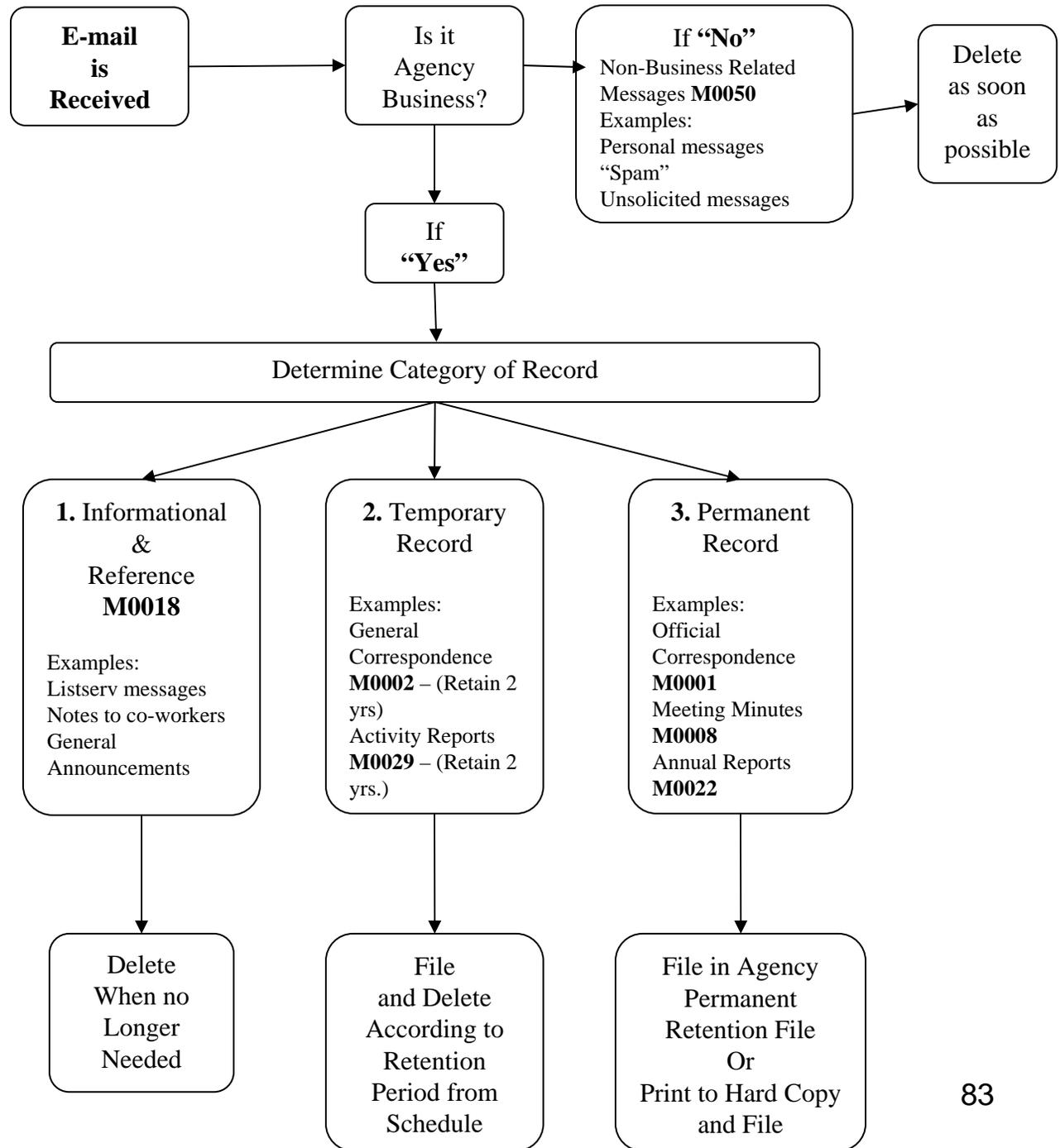
...ATIONS.

Taken from the

Guidelines for Managing Email in KY Government

Located on the KDLA website at:

<http://www.kdla.ky.gov>



Non-business related email

■ Personal Messages

- Needs to be a balance between use and abuse
- Could create risk
 - Viruses
 - Legal liability
 - Embarrassment

■ Spam

- Problems
 - Volume
 - Offensive
 - Viruses

■ Unsolicited E-mail

- A type of spam
- Unwanted e-mail that is work related
 - Advertising from vendors
 - Non-work related e-mail from co-workers
 - Jokes
 - News articles
 - General (Not work related) Announcements



Retaining email messages

- Everyone has email client and capabilities
- Everyone knows how to create messages
- Everyone can forward messages
 - To anyone or everyone
- But do they know how **SAVE** a message properly?

Retaining Email messages

- Move messages out of “In-Box”
- Store messages in a secure location
 - If in on LAN – store on shared drive
 - If on a PC – make sure files are backed up and secure
- If using an ISP or web-based email store messages on local server or hard drive
- If retaining in paper – **Delete the electronic copy!!!**

Sample Filing Structure for E-mail

NON-RECORD MESSAGES – Delete at will

 **Personal Messages**

 **“Spam”/ Unsolicited e-mail**

INFORMATIONAL AND REFERENCE MATERIAL – (M0018) Delete when no longer useful.

 **Drafts** – Publications, Reports, Memos

 **Listserv Messages**

TEMPORARY MESSAGES – Delete per Retention Schedule

 **General Correspondence** (M0002 – delete after 2 years)

 Project 1

 Project 2

 Person A (Supervisor)

 Person B (Co-worker)

 **Activity Reports** (M0029 – delete after 3 years)

 Year #

 Jan, Feb, etc.

 **PERMANENT MESSAGES** – (As defined by retention schedules* Check with agency records officer for appropriate filing procedures.)

 **Official Correspondence** (M0001 – usually from agency or division head)

 Project A

 Project B

 **Annual or Summary Reports** (M0022)

 **Policies and Procedures** (M0003)

 **Meeting Minutes** (M0008)

Retaining email

Email management is a **training problem**, not a technological problem.

E-mail Policy

- Guidelines for acceptable use:
 - Personal vs Business (Use vs Abuse)
- Follow retention periods for the records
 - Delete messages when retention periods expire
- Determine how messages will be retained
 - **Print & File** – Must make sure all information is printed
 - **Electronically** – In central file repository like other electronic records.
- Delete messages that are not business related
- Make sure all employees know and understand the policy

E-mail Policy (Continued)

- Make sure all employees know how to use e-mail
 - Training in how to use the email system
 - Folders
 - Where to store their email
 - Filters/Rules
 - Training in how use email
 - Don't send sensitive/confidential email
 - Restrict personal/casual email
 - Control of copies
 - Email etiquette

Tips for better email management

Send less email!

- CC: and BCC:
 - Often overused
 - BCC: has regulatory issues as well
- Check addressees
 - Don't send messages intended for mark.myers@ky.gov to mark.myers@yahoo.com

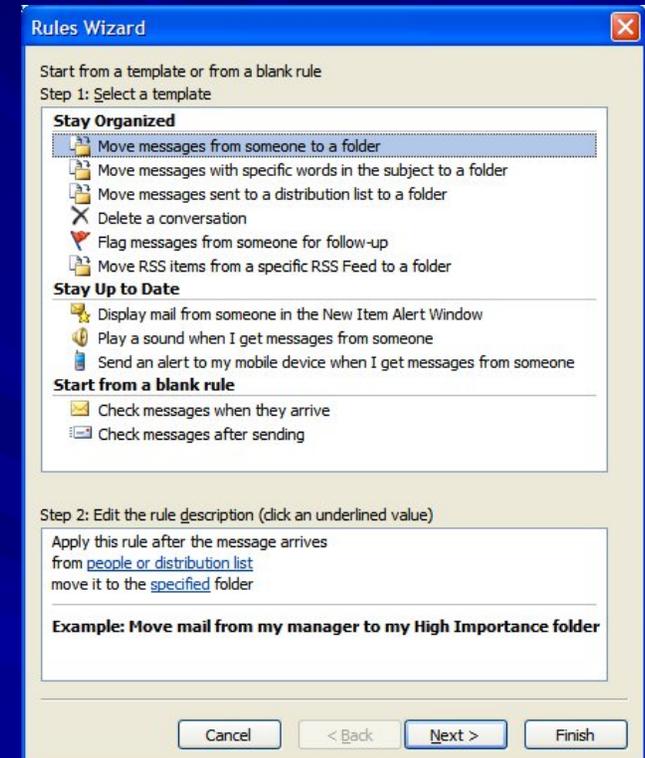
Trim the BACN

- CC: and BCC: again
- A note about bacn
 - Redirect it to folders
 - Redirect it to personal accounts
 - Just get rid of it



4. Set up rules and filters

- Set up rules to direct messages into folders
 - Back
 - Important messages
- Set up filters to forward or block messages
- Use Auto-Archive feature (MS Outlook)



Send good messages

- Keep messages to one topic
- Use appropriate subject line
 - And change it when the subject does
- These make it easier to follow conversations and find messages later
- Don't mix business and pleasure.

Attachments

- Send them only to recipients who really need them
 - Consider file size and formats
- Don't send them at all
 - Send hyperlinks instead
 - Very effective when the organization shifts to links vs. attachments
- Don't use the email app as a file cabinet



Update Email Policy

- Email messages may be records
 - Email is not a record or records series!
- Manage based on content, not based on transmission mechanism
- Check the cord! (blackberries, hand-held devices, mobile computing)



Use the right tool for the job

- Email is not always the right tool
 - Mass updates and announcements
 - Collaboration
 - Public communications
- Select the right tool
 - Blogs, wikis, instant messaging
 - Phone and face-to-face!



Email Guidelines

- *Guidelines for Managing Email in KY Government*

<http://www.kdla.ky.gov/recmanagement/tutorial/email.htm>

- **ARMA (arma.org)**
 - Email Rules
 - **Guideline for Managing Email**
 - Instant Messaging Rules
 - E-Discovery guides

Questions?

Managing Web-based Records

Why worry about Web Records?

- Use of websites is expanding.
- Websites are being used increasingly to display and create official records.
- Interactive and dynamic content will make long-term retention more of a problem.
- The management of these records should be governed by retention schedules

Records found on websites

- General Information
- Publications, Press Releases, Images, “Documents”
 - Original or duplicate copy?
- Transactional records - “E-Business”
- Databases
- Communication – with constituents?
- Is the website itself a record?

Web 1.0

- 1994-2004ish
- Little or no interactivity
- Users had to return to site to look for new content
- Little use of media (audio, video, image files)
- Applications run from your PC
- Web publishers produce and control content

Web 2.0

- 2004ish-now
- Interactivity is the norm
- Users can have content “pushed” out to them
- Lots of use of audio, video, images files
- Applications run on the Web (Gmail, etc.), data & apps in “the cloud”
- Audience produces and controls content (sharing, sharing, sharing)

Managing Web-Based Records

- Analyze web site
 - Identify records on site
 - Risk Assessment of site
- Check schedules for retention period
- Determine best format for retention and capture

Assessing Risk

Factors to consider:

- Public visibility of the site
- Purpose of the web site
 - To convey information
 - To collect information
 - To conduct business (e-government)
- Complexity of the web site
- Frequency and regularity of content change

What makes a high-risk Web site?

- There is high public interest in the Web site
- There is high litigation potential or financial risk
- The Web site is used for mission-critical applications
- Records are not captured elsewhere in agency recordkeeping systems

Other Risk Factors

- Exposure to online attacks
 - Protecting data
 - Protecting users – Your site becomes a weapon
- Timeliness or Inaccuracy of data
- Loss of control of information
- Comments – “Letting the public speak”
 - Inflammatory, Obscene, or just make no sense
 - Responding to comments

The biggest problem(s) . . .

- Personal vs Public
 - When are you not a public official?
- Think about who your “friends” are
 - Who’s linked to you?
 - Who are you linked to?
- Engaging in the debate
 - Be careful what you say
 - Keep it professional
- Can you “play” at work

Web 2.0 tools/sites

- RSS – Really Simple Syndication
- Blogs
- Microblogs - Twitter
- Podcasts (video and audio)
- Image sharing sites - Flickr
- Video sharing sites - YouTube
- Wikis
- Social Networking sites – Facebook, My Space
- Advanced: Social bookmarking, widgets, "mashups," Second Life

Before using Web 2.0 tools

- Who is the media meant to reach?
 - Internal vs External
- What is the agency attempting to communicate?
 - Is this the right tool?
- Who is responsible for managing the agency's account?
 - Will this person/people represent the agency appropriately?
 - Have they been properly trained in the use of social media?
- What are the agency's responsibilities regarding collection and records retention including preservation of social media content?
 - Are these records on the records retention schedule?
- Review the TOS (terms of service)

Develop Social Networking Policy

■ Define scope

- How are you going to use the media

■ Acceptable use

- Personal vs Professional
- Employees need to know the boundaries

■ Clear Identity

- This is a government site
- Company vs Individual

■ Terms of Service (TOS) – Who controls the records

- Records belong to the government
- Read the contract!!

■ Content/Nature of Posts

- Who is allowed to post content
- Clear procedures for putting content online

Social Networking Policy

■ Comments

- Need to make public aware that their post/comments may become part of public record
- Employees need to know same thing

■ Route public to “official” lines of communication

- Point everything back to agency website
- Respond to comments/posts via phone or official email
- Be very careful of people requesting information

■ If you don't have personnel to monitor posts/comments turn them off (if possible).

Social Networking Policy

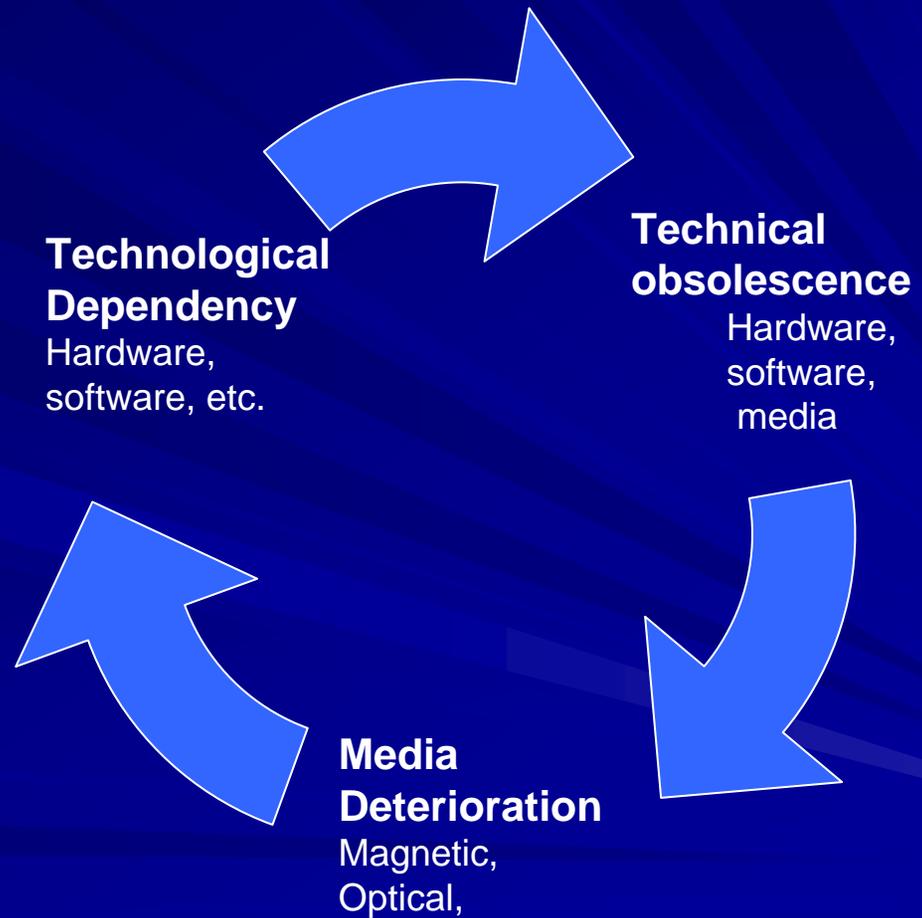
Other issues to consider:

- Don't post confidential information
- Have clear policy for removing posts/comments
- Put someone in charge
- Follow the retention schedules
 - If you have question, contact KDLA

Electronic Records Preservation

Preservation Challenges

- Unlike paper records, digital records do not survive by accident



Terminology

- **Short-term records (0-5 years)**
 - Highly active – on-line storage
 - “Normal” management issues
 - Possible application version upgrade
- **Mid-term records (5-10 years)**
 - Less active – Near-line/Off-line storage
 - Multiple version control issues
 - System upgrades
 - Possible hardware/software migration
- **Long-term records (10+ years)**
 - Least active – Off-line storage
 - Migration/conversion likely

Media Life Expectancy (Physical)

■ Examples

- Paper = 100+ years
- Microfilm = 500 years
- Computer diskette = 2 - 5 years
- DLT = 10 - 30 years
- CD-ROM = 5 - 50 years
- Magneto-optical = 5 - 100 years

Depends on:
Environment
Handling
Media quality

Media Life Expectancy (Actual)

To read a CD-ROM you need:

Hardware

Computer

Disk Drive

CD



Software

Operating System

Driver

Application

Technological Obsolescence



Domesday Book – 1086 CE



BBC Micro Computer

Long-term Preservation Concerns

- Ability to generate in future
- Content, context, structure
- Functionality
- Security

Considerations for Preservation

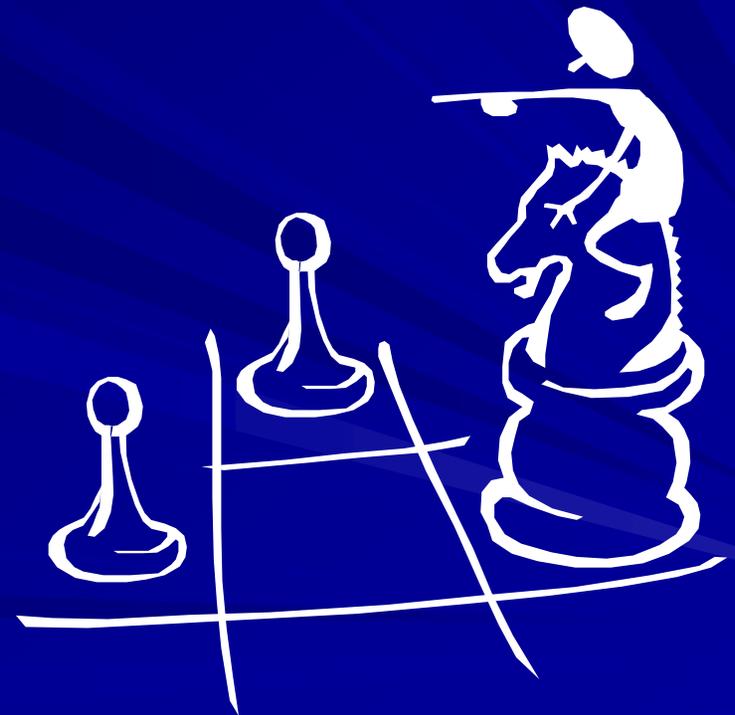
- Perfect translation
- Accessible
- Low cost
- Maintain functionality
- Extensible
- Not labor intensive
- Uniform

Before You Get Started

- Follow appropriate retention schedule(s)
 - Weed records
 - Dispose of obsolete records
- Determine whether to store electronically
 - Do you need to retain the functionality?
 - Do you have the resources?
- Select the appropriate preservation strategy

Long-Term Preservation Strategies

- Conversion to hardcopy
- Standard formats
- Migration
- Emulation



Long-Term Preservation Strategies: Convert to Hardcopy

Best for
“unstructured,”
text-based data:
Word files
Imaged paper
Digital Photos

■ Solution when

- All necessary metadata is captured
- No need to maintain functionality of system
- Frequency of use goes down as time goes on

■ Examples

- Print electronic data to paper
- Digital to Microfilm
- Rosetta disk

Long-Term Preservation Strategies: Standard (Sustainable) Formats

Types of Standards

- Enterprise Architecture
- National/ International Standards (ANSI, ISO)
- Industry Standards
- “De facto” Standards

Formats expected not to change, or change slowly

- Widely supported & used
- Easily Transferable
 - Compatible with other applications
 - Forward/Backward Compatibility
 - Version Control
- Non-proprietary / open source



Standard Formats - Example

The image shows a screenshot of a computer screen with two windows open. The top window is Microsoft Word, titled "Microsoft Word - Active Records Grant Category (2003-2004).doc". The bottom window is Notepad, titled "Active Records Grant Category (2003-2004).txt". The Notepad window displays the following text:

2. Active Records
Records management can have the greatest positive impact when applied to active records. These are among the most important records in a local government because they are used the most frequently, cost the most to maintain, and are essential to the current management of the government.

Activities Eligible for support

a) Files Management supports projects to reorganize paper or electronic files and develop and implement files classification systems, to develop written policies and procedures, and to train staff. Eligible expenditures include file shelving (including that with locking covers), side-tab file folders and associated supplies. Fire-resistant filing cabinets are eligible only if their need is sufficiently justified, but filing cabinets (storage devices with drawers) and top-tab file folders are not eligible.

b) Disaster and Business Recovery Planning supports projects to develop and test disaster and business recovery plans.

c) Indexing and Access supports projects to index or improve access to any active records, including minutes, vital records, or student records. Methods used to improve access might include traditional indexing, implementing full-text searching software, scanning and converting printed text to electronic text, or some combination of these.

d) Imaging and Document Management supports imaging and document management needs assessment and implementation projects. A document management system allows for the creation, indexing, maintenance and retrieval of documents in various formats through a single interface.

e) Geographic Information Systems (GIS) supports GIS needs assessment and implementation projects. The State Archives provides seed money for the initial implementation of GIS in local governments, but does not fund continued improvements to GIS beyond this point.

f) eGovernment supports projects to enhance a government's ability to transact business over the Internet. Governments can propose to conduct needs assessments for website development or enhancement, to provide online access to government records, or to develop systems to file records over the Internet.

g) Electronic Records Systems covers the development of needs assessments or the implementation of any recordkeeping system not covered under another category. Such recordkeeping systems could include database management systems (such as fire incident reporting software), computer output to laser disc (COLD) applications, and many others.

h) Business Process Analysis (BPA) supports the analysis and improvement of business processes that create or maintain records. BPA projects are a good choice for a government that has identified a problem with the way it conducts a specific recordkeeping activity but does not have a specific technological solution to that problem.

Category Requirements
General Technology Project Requirements:
? Records Management Focus. The State Archives does not fund technology projects; it funds records management projects that sometimes have a technology focus. To be eligible for funding, a

The Microsoft Word window shows a table of contents on the left side of the page, with the following entries:

1. Active Records
2. Active Records
3. Active Records
4. Active Records
5. Active Records

The status bar at the bottom of the Notepad window shows "Page 1 Sec 1 1/4 At 1.6" and the date "7/13/2011".

Sustainability Factors for Digital Formats – Library of Congress

- **1. Disclosure.** Degree to which complete specifications and tools for validating technical integrity exist and are accessible to those creating and sustaining digital content. A spectrum of disclosure levels can be observed for digital formats. What is most significant is not approval by a recognized standards body, but the existence of complete documentation.
- **2. Adoption.** Degree to which the format is already used by the primary creators, disseminators, or users of information resources.
- **3. Transparency.** Degree to which the digital representation is open to direct analysis with basic tools, such as human readability using a text-only editor.
- **4. Self-documentation.** Self-documenting digital objects contain basic descriptive, technical, and other administrative metadata.
- **5. External Dependencies.** Degree to which a particular format depends on particular hardware, operating system, or software for rendering or use and the predicted complexity of dealing with those dependencies in future technical environments.
- **6. Impact of Patents.** Degree to which the ability of archival institutions to sustain content in a format will be inhibited by patents.
- **7. Technical Protection Mechanisms.** Implementation of mechanisms such as encryption that prevent the preservation of content by a trusted repository.

<http://www.digitalpreservation.gov/formats/sustain/sustain.shtml>

Long-Term Preservation Strategies: Migration

- Periodic transfer of data to newer system
 - Before old system becomes obsolete
 - Not refreshing (transfer of data to new media)
- Can do item-by-item migration
- Or programmed mass migration
- **Problems:**
 - Often expensive
 - Often time-consuming & labor-intensive
 - Some information loss may occur
 - Must institute time-consuming quality control



Long-Term Preservation Strategies: Emulation

- Allows one technology to imitate another
 - By using new hardware and software
 - Data is stored in original file format
- Complicated and potentially expensive
- Experimental: Needs further investigation

Emulation Examples

- Online game emulators
 - Allow people to play obsolete video games
 - MAME supports a number of old platforms
- Upward compatibility
 - Allows reading of older files in newer software (Word 97 files read in Word XP)
 - Usually lasts only a few software generations
- Macintosh Windows emulation
 - Allows use of Windows programs on a Macintosh
 - Must be rewritten for each new version

Emulation Example: DOS Using Windows XP

The screenshot displays a Windows XP desktop environment. On the left, a File Explorer window is open to the C: drive, showing a tree view of folders and files. On the right, a Command Prompt window is open, showing the output of the 'dir' command.

File Explorer (C:\):

- Local Disk (C:)
 - BACKUP
 - DELL
 - DELLUTIL
 - DISCOVER
 - DMI
 - Documents and Settings
 - DOS
 - DRIVERS
 - I386
 - NALCache
 - NOVELL
 - Oracle
 - Program Files
 - RECYCLED
 - RECYCLER
 - System Volume Information
 - temp
 - unzipped
 - Windows Update Setup Files
 - WINNT
 - YAMAHA
 - Audio CD (D:)
 - Login on 'Cehome\Sys' (F:)
 - Ext on 'Cehome\Usr2\AppData\Oce' (J:)
 - Util on 'Cehome\Usr2\AppData\Oce' (K:)
 - Oce on 'Cehome\Usr2\AppData\Oce' (M:)

Command Prompt:

```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>dir
Volume in drive C has no label.
Volume Serial Number is 447E-D1AA

Directory of C:\

06/20/2002  01:29p    <DIR>          BACKUP
11/16/2001  01:19p    <DIR>          DELL
10/19/2001  12:33a    <DIR>          DELLUTIL
10/19/2001  12:31a    <DIR>          DISCOVER
01/25/2002  03:50p    <DIR>          DMI
06/18/2002  11:43a    <DIR>          Documents and Settings
10/19/2001  12:31a    <DIR>          DOS
10/19/2001  12:34a    <DIR>          DRIVERS
04/30/2002  02:47p                296 g240.txt
10/19/2001  12:31a    <DIR>          I386
06/21/2002  10:42a                202 lconfig.aot
11/16/2001  01:44p                147 localno.log
10/27/2000  02:18p                44 mcafee.txt
11/20/2001  10:01a    <DIR>          NOVELL
11/20/2001  10:20a    <DIR>          Oracle
06/20/2002  01:33p    <DIR>          Program Files
12/12/2001  05:49p                333 Shortcut to WINNT.lnk
11/20/2001  10:08a    <DIR>          temp
06/20/2002  01:35p    <DIR>          unzipped
11/16/2001  01:19p    <DIR>          Windows Update Setup Files
06/21/2002  07:42a    <DIR>          WINNT
04/30/2002  02:37p                1 WINNTNWLogRes.tmp
06/21/2002  07:42a                846 WSREG32.LOG
11/16/2001  01:35p                0 WSREMOTE.ID
11/20/2001  10:02a                546 WT61CE.UWL
11/20/2001  10:02a                546 WT61OZ.UWL
11/20/2001  10:02a                546 WT61UK.UWL
11/20/2001  10:02a                8,198 WT61US.UWL
10/19/2001  12:54a    <DIR>          YAMAHA
05/16/2002  03:53p                70 ZD3WMINU.ct1
13 File(s)                11,775 bytes
17 Dir(s)                17,767,160,320 bytes free

C:\>_
```

Evaluate Preservation Strategies

- Cost effectiveness
- Accessibility
- Necessary functionality
- Newness of strategy



Disaster Preparedness & Recovery

Are you ready?



*That is the
Vital
Question!*

Electronic Records Disaster/Recovery Plan

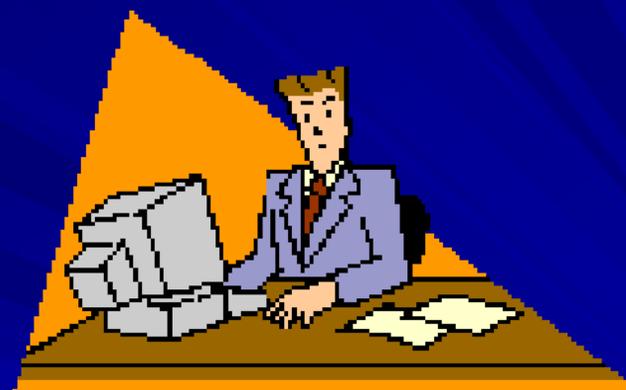
For any loss of service:

■ Dramatic

- Disaster
- Power failure
- Virus or Attack

■ Mundane

- Crashes
- System Failures



Electronic Records Disaster/Recovery Plan

- Firewalls and Network Security
 - Make sure software is up to date
 - Regular updates & patches
 - Test before installing on entire network
 - Password protect all PC's
 - Train employees in proper use of passwords
 - Require log-ins and registration
- Install Anti-virus software
 - Keep it updated!!

Electronic Records Disaster/Recovery Plan

- Back-up all electronic systems
 - Store back-ups off-site
- Mirrored sites
 - Complete duplication of site that takes over when one site goes down.
- Have documentation of everything
 - Hardware/Software documentation
 - Policies and Procedures
 - Inventory of records in system

Questions?

What We've Learned

Advantages,
Disadvantages
&
Lessons Learned

KDLA Approach

- Communication/Collaboration is Key
 - State IT Dept.
 - State/Local Agencies
 - Other States/Federal Gov
 - NHPRC – PAT Project
 - NHPRC – hMail Server
 - NDIIP – GIS Records???

Advantages

- Increased Visibility
 - Increased access to resources
- “Talking the Talk”
- Better understanding of issues
 - Determining the “Business Need”
 - Records as an Asset
 - Legal Issues
- Greater compliance (hopefully)



Disadvantages



- The “Red Tape” got redder
- Inherited each other’s problems
 - Animosity toward central control of IT
 - Legal issues vs everything else
 - Lost in the sea of issues
- Too focused on State issues (over local governments)

Best Advice - “Just Do It!”



- Figure out what you can do and work on it.
 - Exploit your strengths
 - Micrographics/Digital Imaging
 - Publications
- Partner with somebody
 - Collaborative projects
 - Join groups or committees
- Keep it simple
 - Don't reinvent the wheel
 - Look for practical/realistic solutions
- Don't be afraid to get dirty!

Best Advice

- Change is here!
 - Role of records management
 - Legal vs IT vs Business use . . .
 - Arthur Anderson, Enron, etc.
 - Role of archivists
 - Step into the light
 - Distributed custody
 - Volume
 - Formats
 - Access

Future of Electronic Records

- Storage is cheap. . .
- Moving away from “computer”
- Mobile computing – “Blackberry”
- Web 2.0
 - Blogs
 - Flickr
 - You Tube
 - Facebook
- Obama and the future . . .

Questions?

Thank You!



KDLA web site:

<http://www.kdla.ky.gov>

E-mail:

mark.myers@ky.gov

Phone:

(502)564-8300 Ext. 244