MARILYN EDWARDS
County Judge

280 North College, Suite 500
Fayetteville, AR 72701

WASHINGTON COUNTY, ARKANSAS

County Courthouse

September 30, 2016

MEETING OF THE
WASHINGTON COUNTY QUORUM COURT
COUNTY SERVICES COMMITTEE

Monday, October 3, 2016
5:30 P.M.
Washington County Quorum Court Room

Vice-Chair Daniel Balls
Sharon Lloyd
Sue Madison

Chair Eva Madison

Robert Dennis
Tom Lundstrum
Gary McHenry

AGENDA

1. Call to Order.

2. Adoption of Agenda.

3. Bi-Monthly Report from Washington County Planning Office (3.1)

4. An Ordinance Amending Washington County Code Sections 2-62.1 Through 2-62.6 Pertaining To Computer Usage, Electronic Mail And Internet Security Policy. This ordinance was initially presented to the Ordinance Review Committee. Attachments #4.2-4.4 are from Arkansas Department of Information Systems Best Practices and include the Internet Appropriate Use Policy, Password Management, and Electronic Records Management.

5. Public Comments.

6. Adjournment.

/cs

3.1

WASHINGTON COUNTY
QUORUM COURT SERVICES COMMITTEE/PLANNING BOARD
Aug 15, 2016 to Sept 15, 2016
PLANNING DEPARTMENT STAFF REPORT
Juliet Richey, Director

WASHINGTON COUNTY STAFF REVIEWED AND APPROVED THE FOLLOWING ADMINISTRATIVELY:

16 PROJECTS (INVOLVING 25 LOTS)

9 EXEMPTION SPLITS – Total New Lots Created: 18

Planning Area Splits	Lots	County Splits	Lots
Tontitown (2)	4	(3)	6
Fayetteville (3)	6		
West Fork (1)	2		

3 FAMILY SPLITS – Total New Lots Created: 7

Planning Area Splits	Lots	County Splits	Lots
(0)	0	(3)	7

0 CELL TOWER ARRAYS

Planning Area		County
(0)		(0)

4 LOT LINE ADJUSTMENTS

Planning Area		County
Fayetteville (2)		(2)

AT THE SEPTEMBER 08, 2016, PLANNING BOARD / ZONING BOARD OF ADJUSTMENTS MEETING THE FOLLOWING ITEMS WERE HEARD:

Three Conditional Use Permit Hearings were approved:

1. **Maquiladora Manufacturera LLC, USA –** Conditional Use Permit Request. Project is located in Springdale's Planning Area (62.34 acres). Proposed land use: Commercial Welding/Metal Fabrication Shop.

2. **Ingram Residential CUP –** Conditional Use Permit Request. Project is located solely within the County (1.4 acres). Proposed land use: Single Family Residential.

3. **DANCE by Eliese CUP –** Conditional Use Permit Request. Project is located within Fayetteville's Planning Area (1.56 acres, 0.48 acres to be used for the CUP). Proposed land use: Commercial Dance Studio.

Seven Land Development Hearings was approved:

1. **Replat Tract 1 Urban Acres Subdivision –** Preliminary and Final Minor Subdivision Replat Request. Project is located solely within the County (2.91 acres / 2 lots). Proposed land use: Single Family Residential/One non-residential (for access only).

2. **Replat Lot 7 & 8 Brakey Minor Subdivision –** Preliminary and Final Minor Subdivision Replat Request. Project is located solely within the County (4.47 acres / 2 lots). Proposed land use: Single Family Residential.

3. **Replat Lot 33 Tony Mountain Minor Subdivision –** Preliminary and Final Minor Subdivision Replat Request. Project is located solely within the County (5.82 acres / 2 lots). Proposed land use: Single Family Residential.

4. **Replat Lot 30 Tony Mountain Minor Subdivision –** Preliminary and Final Minor Subdivision Replat Request. Project is located solely within the County (16.07 acres / 2 lots). Proposed land use: Single Family Residential.

5. **Cantrell Minor Subdivision –** Preliminary and Final Minor Subdivision Request. Project is located solely within the County (13.97 acres / 4 lots). Proposed land use: Single Family Residential.

6. **Fritchie Farms Large Scale Development** – Final Large Scale Development Request. Project is located in Goshen's Planning area (19.9 acres). Proposed land use: Event Center.

7. **Salem Storage Expansion LSD** – Final Large Scale Development Request. Project is located in Fayetteville's Planning area (8.00 acres / 1 building with 44 storage units). Proposed land use: Storage Units.

One Conditional Use Permit was tabled by the Planning Board:

1. **White River Landing CUP –** Conditional Use Permit Request. Project is located in Greenland's Planning Area (10.31 acres). Proposed land use: Wedding/Event Center.

Two Conditional Use Permits were tabled (at the request of the applicants):

1. **Meadows at River Mist CUP –** Conditional Use Permit Request. Project is located solely within the County (59.75 acres / 155 lots). Proposed land use: Residential Subdivision.

2. **Mountain Cars CUP –** Conditional Use Permit Request. Project is located within Greenland's Planning Area (0.68 acres). Proposed land use: Commercial Car Lot.

One Land Development was tabled (at the request of the applicants):

1. **Meadows at River Mist LSD –** Preliminary Subdivision Request. Project is located solely within the County (59.75 acres / 155 lots). Proposed land use: Residential Subdivision.

THE OCTOBER 06, 2016, PLANNING BOARD / ZONING BOARD OF ADJUSTMENTS MEETING WILL CONSIST OF THE FOLLOWING:

Two Conditional Use Permit Hearings:

1. **Meadows at River Mist CUP –** Conditional Use Permit Request. Project is located solely within the County (59.75 acres / 155 lots). Proposed land use: Residential Subdivision.

2. **Huntsville Road Storage CUP –** Conditional Use Permit Request. Project is located within Fayetteville's Planning Area (4.22 acres). Proposed land use: Commercial Storage.

Four Land Development Hearings:

1. **Meadows at River Mist LSD –** Preliminary Subdivision Request. Project is located solely within the County (59.75 acres / 155 lots). Proposed land use: Residential Subdivision.

2. **Huntsville Road Storage LSD–** Preliminary Large Scale Development Request. Project is located within Fayetteville's Planning Area (4.22 acres). Proposed land use: Commercial Storage.

3. **Rose Subdivision –** Preliminary and Final Minor Subdivision Replat Request. Project is located solely within the County (6.54 acres / 6 lots). Proposed land use: Single Family Residential.

4. **Replat PT Lot 113 Wedington Woods (Unit 1) Subdivision –** Preliminary and Final Minor Subdivision Replat Request. Project is located solely within the County (22.70 acres / 1 lot). Proposed land use: Single Family Residential.

4.1

Karen\Computer Usage Code Sec 2-62.1 thru 2-62.6 ord 08/08/16

ORDINANCE NO. 2016-_____

**BE IT ORDAINED BY THE QUORUM COURT
OF THE COUNTY OF WASHINGTON,
STATE OF ARKANSAS, AN ORDINANCE
TO BE ENTITLED:**

AN ORDINANCE AMENDING WASHINGTON COUNTY CODE SECTIONS 2-62.1 THROUGH 2-62.6 PERTAINING TO COMPUTER USAGE, ELECTRONIC MAIL AND INTERNET SECURITY POLICY.

WHEREAS, in 2002 the Quorum Court passed a policy concerning computer usage, electronic mail, and internet security policy; and,

WHEREAS, due to the passage of time and changes in technology such policy needs to be updated; and,

WHEREAS, though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions;

WHEREAS, this access carries certain responsibilities and obligations as to what constitutes acceptable use of the county network; and,

WHEREAS, County Employees and Elected Officials are obligated to use, conserve and protect electronic information and County information technology resources for the benefit of the County and its taxpaying citizens.

NOW, THEREFORE, BE IT ORDAINED BY THE QUORUM COURT OF WASHINGTON COUNTY, ARKANSAS:

ARTICLE 1. Washington County Code Sections 2-62.1 through 2-62.6 are hereby repealed and replaced with the following:

2-62.1 Information Technology Resources Defined.

"Information Technology Resources" consist of all electronic communication assets and equipment, hardware, software, systems, services, networks, data and peripherals owned, leased, rented, established, controlled or otherwise administered by Washington County. These assets enable individuals to access or interact with information stored on or transmitted within the County data network, telecommunication systems, cellular systems and other internal or external sources. These resources include, but are not limited to the following: antivirus systems, cellular devices, control systems, card entry systems, cellular services, copiers, credit card readers, data backup systems, data racks, data transmission, cables, desktop computers, desktop printers, digital cameras, digital tape drives, distribution lists, electronic data, electronic documents, electronic images, electronic mail messages, electronic mail systems, FAX machines, fiber optic systems, financial systems, firewalls, hubs, internet services, intranet services, label printers, laptop computers, large format printers, laser printers, mobile telephones, modems, monitors, network bandwidth, network cabling, network security cameras, network security services, operating systems, point of sale devices, point of sale systems, projectors, personal communication devices, records management systems, remote access systems, routers, scanners, server racks, servers, software applications, social media accounts, surge protectors, switches, tablet computers, telephone services, telephone systems, telephones, televisions, text messages, USPs, USB drives, utility systems, voicemail systems, VPN systems, websites, and wireless access points.

2-62.2 Expectation of Privacy; Prohibited Use; Regulations Authorized.

(a) There is no legitimate expectation of privacy in electronic communication or data stored on or in County Information Technology Resources, and all such communication or data shall be subject to disclosure in accordance with the Arkansas Freedom of Information Act (ARK. CODE ANN. § 25-19-101 through 110, as amended), and other applicable law. Provided however, that this subsection does not mandate the disclosure of information deemed “law enforcement sensitive” or that is protected by applicable professional confidentiality or privilege.

(b) Upon the receipt of credible information that any authorized user of County Information Technology Resources is using, has used or is attempting to use County Information Technology Resources in the planning, attempt, commission or furtherance of any criminal act as defined by International, Federal, State, or local law, the County Information Technology Office is authorized to immediately suspend the authorized user’s access to County Information Technology Resources, pending further investigation.

(c) Upon conviction by a court of competent jurisdiction of any authorized user of County Information Technology Resources of any criminal act, including, but not limited to, substantive and inchoate offenses as defined by International, Federal, State, or local law, the County Information Technology Office is authorized to permanently terminate the authorized user’s access to County Information Technology Resources.

(d) Upon receipt of credible information that any authorized user of County Information Technology Resources has intentionally breached or tested the security of County Information Technology Resources, or that an authorized user of County Information Technology Resources has intentionally damaged or destroyed County Information Technology Resources, the County Information Technology Office is authorized to

(e) immediately suspend the authorized user's access to County Information Technology Resources, pending further investigation. Upon the conclusion of said investigation, if the investigation substantiates an intentional breach, test, damage to or destruction of County Information Technology Resources, the County Information Technology Office is authorized to permanently terminate the authorized user's access to County Information Technology Resources.

(f) This section is not intended, and shall not be construed, to limit the ability of the Washington County Sheriff's Office to investigate and prevent crimes involving information technology. This section is further not intended, and shall not be construed, to limit the Prosecuting Attorney's Office, the Public Defender's Office or any of the Circuit Judges or their respective staffs from using County Information Technology for legitimate job-related activities.

ARTICLE 2. The County Judge, as custodian of county property, in accordance with ARK. CODE ANN. § 14-14-1102 and pursuant to his or her authority to enact administrative rules and regulations on matters within the Judge's capacity as County Chief Executive Officer in accordance with ARK. CODE ANN. § 14-14-1104, is hereby authorized to promulgate such rules and regulations as are reasonable and necessary to protect, secure, safeguard, promote the efficient use of and conserve County Information Technology Resources, and the same shall be binding upon all authorized users of County Information Technology Resources.

______________________________	______________________________
MARILYN EDWARDS, County Judge	DATE

____
BECKY LEWALLEN, County Clerk

Sponsor:_________Bill Ussery_____________
Date of Passage:________________________
Votes For:________ Votes Against:_________
Abstention:_______ Absent:_________

- Title of Agency -

Internet Acceptable Use Policy

The Following Internet Acceptable Use Policy Applies to the (AGENCY NAME) Staff

1. Introduction

The *(AGENCY NAME)* provides its staff and *(other entity(s) if necessary)* with technology resources and a local area network with access to the Internet. The purpose of these technologies is to: a) enhance the programs and services provided by *(AGENCY NAME)*, b) conduct (*AGENCY NAME*) business, c) support *(AGENCY NAME)* projects, and d) ensure that staff are equipped with the necessary tools for communication, research, collaboration, and other tasks required to fulfill job obligations. Each staff member is expected to use accounts and resources for these purposes.

- Currently, each *(AGENCY NAME)* staff member has been provided adequate resources for Internet connectivity. The staff relies on this connectivity in order to adequately perform their job duties and responsibilities.
    - The *(AGENCY NAME)* provides approximately ___ employees access to a networked computer. This represents (_____) % of the employees in the agency.
- All *(AGENCY NAME)* staff must carefully review and adhere to these Internet acceptable use guidelines.

2. Appropriate Use of Technology

2.1. Technology as a required resource and privilege

Appropriate uses of technology include:

- Accessing the Internet for work related research and information gathering;
- Utility and applications software that accomplish tasks and fulfill job functions;
- Communication and collaboration between staff and/or other appropriate entities;
- Access to the Internet for up-to-date information published by *(AGENCY NAME)*, other state agencies, and various other providers of information that may be necessary in order to complete job tasks;
- Activities or projects that support professional activities of employees (i.e., electronic calendars, electronic scheduling of meetings, electronic prioritizing of tasks, using project management software, keeping electronic address books, and completion of work related forms electronically)

2.2. Privacy of Information

(AGENCY NAME) reserves the right to monitor and/or log all network activity with or without notice, including e-mail and all web site communications, and therefore, users should have no expectation of privacy in the use of these resources.

- The Agency will not monitor e-mail transmissions on a regular basis, though the construction, repair, operations and maintenance of electronic messaging systems may occasionally result in monitoring random transmitted or stored messages.
- Messages may be monitored during the course of investigations of illegal activity.

- The agency will not provide third parties with access to stored electronic messages without the written consent of the sender and recipient except in special circumstances, such as investigating illegal activity or misuse of the system, or resolving a technical problem.

2.3. Governor's Policy Directive

Governor's Policy Directive GPD-5, 1997 clearly states that... "Use of any and all State-owned equipment and supplies shall be restricted to official state use only. Unauthorized or personal use of equipment or supplies may be grounds for dismissal."

2.4. User Restrictions

(AGENCY NAME) staff will not excessively use the agency network, computer systems, and servers including access to the use of the Internet and other information resources during regular office hours for non-agency business. Limited personal use of these resources is allowed during breaks and lunch time, or to address critical personal matters.
Only games that are part of the workstation's operating system will be permitted to be used during normal break times and only without sound features activated.

2.5. Unacceptable Uses

The following general uses are prohibited:

- Interference with the security or operation of the computer systems;
- Vandalizing equipment, software, or hardware;
- Attempting to alter or gain access to unauthorized files or systems;
- Using technology in a way that interferes with work obligations;
- Violating the rights of others by publishing or displaying any information that is defamatory, obscene, known to be inaccurate or false, profane, or threatening.
- It is unacceptable for a user to use, submit, publish, display, or transmit on the network or on any computer system any information which:
  - Violates or infringes on the rights of any other person, including the right to privacy;
  - Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
  - Inhibits other users from using the system or the efficiency of the computer systems;
  - Encourages the use of controlled substances or uses the system for the purpose of criminal intent;
  - Uses the system for any other illegal purpose.
- It is also unacceptable for a user to use the facilities and capabilities of the system to:
  - Knowingly transmit material, information, or software in violation of any local, state or federal law;
  - Conduct any non-governmental-related fund raising or public relations activities;
  - Engage in any activity for personal financial gain, such as buying or selling of commodities or services with a profit motive;
  - View, download or send pornographic or other obscene materials;
  - Visit and/or participate in chat rooms not designed for professional interactions specifically related to one’s job;
  - Endanger productivity of *(AGENCY NAME)*.

3. Electronic Mail (E-mail)

E-mail is considered network activity and as such is subject to all policies regarding acceptable/unacceptable uses of the Internet. The user should not consider e-mail to be either private or secure.

3.1. Purpose of E-mail

Electronic mail is provided to support open communication and the exchange of information between staff and other authorized users that have access to a network. This communication allows for the collaboration of ideas and the sharing of information. E-mail is a necessary component of teamwork at *(AGENCY NAME)*.

3.2. E-mail Guidelines

Each *(AGENCY NAME)* staff member is given an E-mail account. It is the responsibility of the employee to use their account in accordance with established guidelines and in such a way that does not interfere with their duties.

Specifically prohibited in the use of e-mail is:

- Any activity covered by inappropriate use statements included in this policy;
- Sending / forwarding chain letters, virus, hoaxes, etc.;
- Sending, forwarding or opening executable files (.exe) or other attachments unrelated to specific work activities, as these frequently contain viruses;
- Use of abusive or profane language in messages;
- Submitting any large, unnecessary mail attachments;
- Use that reflects non-professional image of *(AGENCY NAME)*.

3.3. E-mail Storage

Staff should move important information from E-mail message files to shared folders and drives to ensure proper backup. Messages no longer needed must be periodically purged from personal storage areas. Technical support staff will monitor storage usage and advise when limits are reached and purging is required.

4. Internet

4.1. Purpose of Internet Access

The Internet provides a wealth of information useful for educational purposes. With Internet access an employee of *(AGENCY NAME)* can utilize the many research and resource tools available online. These tools can aid in preparing reports or projects required by the agency.

All *(AGENCY NAME)* staff members may access the Internet and other information resources and services at any time that in the judgement of the user, such access and use will benefit *(AGENCY NAME)* programs and services.

4.2. Internet Access Guidelines

When online, employees should abide by conventional etiquette guidelines developed for the Internet (‘netiquette’).

4.3. Appropriate Use of Web Access

Employees are responsible for making sure they use this access correctly and wisely. Staff should not allow Internet use to interfere with their job duties.

Acceptable uses include:

- Access to and distribution of information that is in direct support of the business of *(AGENCY NAME)*.
- Providing and simplifying communications with other state agencies, school districts and citizens of Arkansas;
- Communication of information related to professional development or to remain current on topics of general *(AGENCY NAME)* interest;
- Announcement of new laws, rules, or regulations;
- Encouraging collaborative projects and sharing of resources.

Inappropriate uses of web access include, but are not limited to:

- Viewing, downloading or sending pornographic or other obscene materials;
- "Surfing" the Web for inordinate amounts of time;
- Otherwise endangering productivity of *(AGENCY NAME)*.
- Purposes which violates a Federal or Arkansas law;
- Dissemination or printing copyrighted materials (including articles and software) in violation of copyright laws.

5. Appropriate Network Use and User Accounts Guidelines

Use of the state's Internet connection and E-mail resources is a privilege and it is expected that all staff abide by acceptable user guidelines. Appropriate network and user account guidelines include:

- *(AGENCY NAME)* staff will only access those computer accounts which have been authorized for their use and must identify computing work with their own names or other approved IDs so that responsibility for the work can be determined and users can be contacted in unusual situations.
- *(AGENCY NAME)* staff will use accounts for authorized purposes. This policy shall not prevent informal communication, but accounts will not be used for private consulting or personal gain.
- Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Staff should not expect files and documents to always remain private.
- Users are encouraged to maximize the use of the technologies covered under this user policy to reduce the cost of postage, letters, reports, etc.

6. Copyright Guidelines

6.1. Purpose of Software Availability

(AGENCY NAME) provides utility and application software that enhances the efficiency and productivity of its employees. *(AGENCY NAME)* staff must honor copyright laws regarding protected commercial software used at the agency.

6.2. Compliance With Copyright Laws

- Copyright laws do not allow a person to store copies of a program on multiple machines, distribute copies to others via disks or Internet, or to alter the content of the software, unless permission has been granted under the license agreement.
- Users may download copyrighted material, but its use must be strictly within the agreement as posted by the author or current copyright law.
- Unauthorized use of copyrighted materials or another person's original writing is considered copyright infringement.

- Any user that copies and distributes software in any form for any purpose should do so only on the authority of the user's immediate supervisor.
- Each user is responsible for observing all local, state, federal laws, especially in regard to copyright laws. The agency will not be responsible for the cost of any legal action taken against any user that violates such laws regardless of the situation or the intent or purpose of the user.
- All staff that use software owned by *(AGENCY NAME)* or the state must abide by the limitations included in the copyright and license agreements entered into with software providers.

7. Enforcement and Penalties

The *(AGENCY NAME)* staff is responsible for complying with this policy. Penalties for non-compliance include, but are not limited to:

- Suspension or usage restrictions of Internet service and email/messaging services.
- Internal disciplinary measures, including discharge.
- Initiation of criminal or civil action, if appropriate.

Internet Acceptable Use Policy Consent Form

(AGENCY NAME)

I ____________________________ have read this policy and agree to comply with all its terms and conditions. Furthermore, I ____________________________ understand that the *(AGENCY NAME)* will not monitor e-mail transmissions on a regular basis, though the construction, repair, operations and maintenance of electronic messaging systems may occasionally result in monitoring random transmitted or stored messages.

(AGENCY NAME) users must recognize that the use of all *(AGENCY NAME)* and state electronic information resources necessary to conduct agency business, and that the policies implementing usage, are requirements that mandate adherence.

Signed: ____

Date: ____

Supervisor: ____

Date: ____

State of Arkansas

Best Practices Statement – K-12 Password Management

Title: K-12 Student Password Management

Document Number: BP-70-011

Effective Date: 12/16/08

Published by: Department of Information Systems

1.0 Purpose

Passwords are the most common way to allow access to computer systems and it is important to use a hard to guess password to prevent unauthorized access.

2.0 Scope

This best practices statement is recommended for students in the K-12 schools enrolled in the 4th grade and older.

3.0 Background

Act 723 of 2007 gives the Arkansas Department of Education the authority to implement policies to provide for data quality and security with the Arkansas Public School Network. In support of the Department of Education, the Department of Information Systems has developed password best practices for the K-12 students enrolled in the 4th grade and older.

4.0 References

4.1 Act 723 of 2007: An Act to Provide for Improved Processes to Ensure the Quality, Security, Validation, and Timeliness of Public School Data in the Arkansas Public School Computer Network

4.2 Act 751 of 2007: Authorized the Department of Information Systems to develop security policy.

5.0 Best Practices Recommendation

5.1 Passwords for access to school and educational service cooperative networks and applications containing sensitive and/or confidential information should be:

5.1.1 At least eight characters in length with a mixture of alpha and nonalpha characters
5.1.2 Changed a minimum of every semester

5.2 K-12 students with elevated access should utilize passwords that comply with the state password management standard (SS-70-002).

6.0 Definitions

6.1 Password:
A secret word or code used to serve as a security measure against unauthorized access to data or systems.

Practical Approaches to Electronic Records Management and Preservation

Developed by the Arkansas Information Architecture Working Group

November - 2001

For More Information Contact Drew Mashburn
Office of Executive Chief Information Officer: 501-682-5256

Table of Contents

Overview:

The Arkansas Enterprise Information Architecture Group[1] has developed draft guidelines for state agencies to use in the management of electronic records. These practical approaches are intended to guide agencies toward developing effective records management procedures. The practical approaches to managing electronic records described in Part I includes: 1) creating, and managing electronic records; 2) protection and preserving electronic records; 3) proper disposal; 4) collection and use of personal information; 5) agency Internet web site privacy statements; 6) maintaining secure, reliable and trustworthy systems; 7) electronic records correspond to business needs; and 8) three functional requirements to ensure effective electronic record keeping.

Part II (E-mail Guidelines) addresses E-mail as a public record. The purpose of Part II is to assist agencies in the management of electronic mail (e-mail) messages as public records within Arkansas state government.

Part III (Electronic Imaging Guidelines) is designed to identify critical issues for agency officials to consider in designing, selecting, implementing, and operating digital imaging technologies. The guidelines provide recommendations and are not intended to serve as a rigid set of requirements. However, the degree to which they are incorporated into system design will greatly effect the long-term accessibility of the electronic records involved.

Part I: Electronic Records Management

Introduction:

The widespread use of technology to conduct government business has resulted in an increase of electronic state records. With the implementation of electronic signatures and the evolution from paper record keeping to electronic records, new requirements for the collection, storage, and long-term retention of records in digital form are emerging. New requirements being proposed in the Freedom of Information Act (FOIA) for custodial responsibilities within agencies and access by citizens to electronic records depend upon standards that will support open access while at the same time consider confidentiality requirements. If this information is mishandled, electronic records can easily be lost or misplaced, and information may be difficult to retrieve. The results are costly delays, lost business opportunities, frustrated office personnel and managers being forced to make decisions based on inadequate information.

Currently, most electronic information systems used to create, receive, and store these public records do not provide full records management functionality. Agencies need to adopt electronic information systems that provide proper controls over the creation of records, maintenance of records, and disposal according to approved processes for managing both open records and confidential record retention schedules.

Statement of Benefit:

The implementation of sound record management practices for electronic records can result in a number of benefits for government. One of the more important benefits is

[1] The Information Architecture Working Group consists of representatives from a variety of Arkansas state agencies.

to ensure the creation and management of accurate and reliable electronic records. This allows agencies to fulfill legal mandates regarding the protection of their records. Other agency benefits include: ensuring the legal acceptability of agency electronic records, reducing costs for the retrieval of records no longer needed to be maintained on the system, reducing the burden of paper record keeping, identifying appropriate means for the movement of records to successive generations of technology and systems and improves citizen access to public information.

Meaning of Terms:

Public records means writings, recorded sounds, films, tapes, electronic or computer-based information, or data compilations in any form medium, required by law to be kept or otherwise kept, and which constitute a record of the performance or lack of performance of official functions which are or should be carried out by a public official or employee, a governmental agency, or any other agency wholly or partially supported by public funds or expending public funds. All records maintained in public offices or by public employees within the scope of their employment shall be presumed to be public records. "Public records" does not mean software acquired by purchase, lease, or license. (From AR Act 1653, An Act to Amend Various Provisions of the Freedom of Information Act; 83rd General Assembly)

Public records include: cards, papers, correspondence, disks, tapes, maps, memoranda, electronic mail, papers, photographs, recordings, reports, microfilm, and optical disks.

Public records are information that is created or received in fulfillment of government work and is therefore subject to records management statutes. It is the complete set of documentation required to provide evidence of a business transaction.

Over the past few years, questions have been raised about the difference between paper versus electronic records. For example: "How long do we have to keep correspondence we've received in the mail versus how long we have to keep our electronic mail?" There is no difference. It does not matter in which form the correspondence was received, paper through the U.S. mail or electronically via the Internet. The record is still "correspondence" and the retention period is the same.

There is a common misconception that the Arkansas Freedom of Information Act (FOI) is a retention statute. The Arkansas FOI law states that if one receives a request for public information, and the request falls within the definition of a public record, and it is not covered by one of the exemptions, then the agency has to make it available. Only retention statutes require one to retain, and Arkansas does not have a general retention statute requiring public servants to retain 'records'. However, there are statutes within the Arkansas Code that require particular government entities to retain particular records (e.g., cities retaining invoices for accounting purposes, court records being retained forever, etc).

Arkansas Code 5-54-121, "Tampering with a Public Record": This Arkansas Code makes it a crime (class D misdemeanor) to destroy a public record; "a person commits the offense of tampering with a public record if with the purpose of impairing the legibility of a public record he knowingly makes a false entry in or alters a public record or erases, removes, destroys or conceals a public record." Therefore, just because one destroys, a 'record' that the Arkansas FOI law does not require be retained, the action of destruction has not violated this statute. However, if one destroys a 'record' that fits under a specific retention law and the destruction of it prevents if from being available, the law has been violated.

State agencies means all state departments, boards, commissions, and institutions of higher learning but shall not include the elected constitutional officers and their staffs, the General Assembly and its committees and staffs, or the Supreme Court and the Administrative Offices of the Courts. State agencies are subject to Arkansas records management statutes.

Custodian: With respect to personal information, it means the person having administrative control of that information (record), or his or her designee. "Custodian" does not mean a person who holds public records solely for the purposes of storage, safekeeping, or data processing for others.

Personal Information is any information that by some specific means of identification, including but not limited to any name, number, description, finger or voice print or picture, and including any combination of such characters, it is possible to identify with reasonable certainty the individual to whom such information pertains.

Practical Approaches to Electronic Records Management and Preservation:

1. Creating and Managing Electronic Records

   Government agencies need to create, manage, and maintain electronic records that are:

   - Accessible over time for business and secondary uses
   - Reliable and authentic (to stand up in legal and business forums)
   - Usable for multiple purposes

Unfortunately, many traditional information system designs do not give adequate attention to the creation, integration, management, and preservation of electronic records. In many cases, redundant paper systems must be maintained or substantial additional resources must be spent in order to address records management requirements after information systems have been implemented.

   a. Maintain adequate search and retrieval capabilities to ensure that electronic records can be retrieved for all legitimate business purposes for their full retention period. This will require adequate indexing as well as search tools.
   b. Develop methods to provide public access to electronic records and to protect personal privacy and confidentiality. When systems are designed, government agencies should develop methods of access that take into account the public access and confidentiality requirements. The need for public access to electronic records must constantly be weighted against a government agency's duty to protect personal privacy and confidentiality.

2. Protection and Preserving Electronic Records

Public managers have an obligation to preserve the integrity of electronic information for current and future uses. As a general rule, only the custodian with authority may destroy an electronic record. Arkansas statutes rest on the premise that public servants have a special obligation to preserve and make accessible a clear record of what they do and make accessible relevant informational data. Agencies have the responsibility to protect records and deliver them to a successor to assure smooth transition and continuity.

a. Principles of Data Protection: Agencies processing personal data should abide by the following eight principles of good practice. The data must be:
   i. Fairly and lawfully processed
   ii. Processed for limited purposes
   iii. Adequate, relevant and not excessive
   iv. Accurate
   v. Kept according to law but not kept longer than necessary
   vi. Processed in accordance with the data subject's rights
   vii. Secure
   viii. Not transferred without adequate protection

3. Records Value to Agency and Citizens

Just as with paper records, the e-records a government agency produces or receives are not all of equal importance or value. Although all government records should be maintained properly, the effort and resources a government agency expends to manage and maintain records, including e-records, should be related to the records' value to the agency and the citizens it serves. Risk management could be used to determine the value of e-records. In applying risk management to electronic records, the following questions should be asked.

a. What would be the impact on agency operations if the records were lost or otherwise unavailable?
b. Would the agency or others suffer a financial loss if the records were unavailable?
c. What is the likelihood that the records would be subject to or needed for a legal action?
d. Are the records required for an extended period of time?
e. Do the records have significant cultural or historical value?

4. Proper Disposal of Records According to Type

Although agencies must keep records, this does not mean all records must be retained permanently. Government data custodians have a responsibility to dispose of data when it is determined to be unnecessary by following appropriate state and federal laws.

5. Collection and Use of Personal Information

The use of personal information collected, stored, or disseminated by government for purposes other than those purposes to which a person knowingly consents can endanger a person's right to privacy and confidentiality.

a. Personal information should be:
    i. Collected, used and maintained only as expressly authorized by law and for legitimate public purposes;
    ii. Relevant to and used only for the specified purpose for which it was originally collected;
    iii. Used only if accurate and up-to-date;
    iv. Kept secure; and
    v. Retained only as long as necessary and then destroyed.

b. There is current debate concerning selling and releasing personal information for commercial purposes. Both federal and state laws can impact policies and practices addressing these issues. Consequently, agencies should be cognizant of any related legal developments.

c. The ability to electronically store, retrieve, and aggregate information raises new concerns about the potential for personal information to not only be accessed, but mined and distributed, as well.

d. Agencies collecting, maintaining or using personal information, under its control, should take precautions to prevent its misuse. It may be an unwarranted invasion of personal privacy for an agency to make personal information available to the public.

e. Social Security numbers, bank account numbers, and credit card numbers should be confidential and should be redacted from any record that could be subject to public scrutiny. State agencies should abide by existing laws prohibiting such information from being released.

f. Several states have authorized by law that personal information shall not be shared among government entities without the consent of the affected individuals. Some state laws mandate that agencies that enter into contracts or agreements for sharing personal information with other entities must have contractual requirements that protect the information from inappropriate uses.

g. Several states have mandated by law or policy that when personal information about individuals is collected, the individuals shall be notified by the collecting agency that the law may require public disclosure of the information, or its dissemination to other agencies, through the state's open/public record laws or by court order. If personal information is collected via e-mail and Web-based forms, laws and/or policies may exist for an individual to opt-out from having their personal information shared with another party, and/or allowing the individual to access their personal information and correct the same.

h. Agencies should establish procedures and practices for handling and the disposal of records that contain personal information so information is not misused.

6. <u>Agency Internet Web Site Privacy Statements</u>
Agencies that operate Internet Web sites should have privacy policies that are prominently displayed on their home pages. The policies must be consistent with regulations developed by the state Executive Chief Information Officer (CIO). At a minimum, agency Web sites that require an individual to enter the following

information should use appropriate encryption technologies to protect the data during transmission:

a. The individual's name and other personal information, such as a social security number;
b. Transaction payment information; and
c. An individual's identification code and password.

7. Maintaining Secure, Reliable and Trustworthy Systems

The acceptance of electronic records for legal, audit, and other purposes is contingent on establishing their authenticity and reliability by demonstrating the trustworthiness of the system used to produce them. Systems that produce records must be shown to do so in the normal course of business and in an accurate and timely manner. The following suggestions should assist record keepers in their efforts to maintain authentic and reliable electronic records that can be successfully used for these purposes.

a. Test system performance including the reliability of hardware and software. The reliability of hardware and software affects the authenticity and integrity of electronic records. Equipment malfunctions can alter the content of these records. If data processing equipment and software used to store and produce electronic records is not reliable, the integrity of the records may be challenged.
b. Develop a contingency plan that includes data backup, disaster recovery, and emergency operations. Contingency plans can help agencies quickly put back into operation systems after a disaster. The plans should include data backup and recovery to prevent the loss of electronic records.
c. Perform routine backups. It is critical to backup software and data especially if that data constitutes e-records. Frequency of backups will depend upon how often data changes and the importance of those changes. Program managers should be consulted to determine what backup schedule is appropriate. Backup copies should be tested to determine if they are usable and stored securely at a location away from the system in the event of a disaster.
d. Maintain physical and environmental security controls. Physical and environmental threats can have an impact on electronic records, especially those stored on fragile offline media. An agency's security program should address physical access and appropriate environmental conditions in office space, data centers, or rooms containing hardware, system wiring, backup media, and any other system.
e. Provide for identification and authentication to ensure the security of electronic records. These would be technical measures that are designed to prevent unauthorized people from entering a system. The system should be able to identify and differentiate users through a unique user identification (ID). The IDs should belong only to currently authorized users. Authentication is the means of establishing the validity of a user's identity.
f. Implement media controls. Some measures include standard labeling and maintaining tracking logs, providing physical and intellectual control over

tapes, diskettes, and other media. Offline media should also be stored in environmentally and physically controlled locations. The extent of media control depends upon many factors, including the type of data, the quantity of media, and the nature of the user environment. Media used to store critical or high-risk e-records will normally demand higher-levels of control than other data.

g. Records in electronic format are hardware and software dependent. These records can only be read and understood if the storage medium can be read by existing equipment and if the programs used to create the digitized data are still available. Data conversions may need to occur.

h. With the shift from mainframe applications to individual and networked personal computers, the risk of data loss increases and the likelihood of regular migration decreases. Desktop users need to be aware of necessary documentation procedures to ensure that data can be read in the future.

i. Computer hardware and software acquired by public entities should not inhibit access to public records (e.g., agencies should make sure that software they acquire has adequate reporting capabilities to permit FOIA compliance and not restrict).

8. Electronic Records Correspond to Business Needs

Implementing sound electronic record keeping represents more than the basic maintenance of electronic data. It also refers to the development and implementation of good management structures that supports organizational record keeping requirements corresponding with business needs. As records are created or captured they are identified to support the business process.

9. Three Functional Requirements To Ensure Effective Electronic Record Keeping:

There are three functional requirements to ensure effective electronic record keeping:

- Records Capture Requirement: The records are created or captured and identified to support the business process and meet all record keeping requirements related to the process.
- Records Maintenance and Accessibility Requirement: Electronic records are maintained so that they are accessible and retain their integrity for as long as they are needed and required by law.
- System Reliability Requirement: A system and its disaster recovery system are administered with best practices in information resource management to ensure the reliability of the records it produces.

Part II. Electronic Mail Management

Introduction

Electronic mail systems, commonly called e-mail, are becoming the communications method of choice for many public officials and public employees in Arkansas. Electronic mail (e-mail) is an information transfer system that utilizes computers for sending and receiving messages. E-mail is often used as a substitute for a phone call but has the same potential evidentiary value as any other record documenting the transaction of public business. Like the telephone, it is specifically intended to handle communications ranging from those immediately discardable, to those worthy of retention. However, e-mails have characteristics of a document (and not a phone conversation) in that they remain in existence after the communication ends. E-mail is also similar to postal mail because a message sent or received by e-mail is documented, "written" onto an electronic medium at the time of transmission, and can be stored for later retrieval or reproduction. This combination of communication and record creation/keeping has created confusion regarding the concept that e-mail messages are records.

The need to treat electronic mail as records for capture, preservation, and management is rapidly growing in importance for the following reasons:

- Messages are getting longer, and contain more information. As the technology advances and users get more comfortable with e-mail, their messages tend to gradually grow from simple messages to actual documents.
- Increases in important decisions, which always constitute valuable records, are being recorded and distributed in exclusively e-mail form.
- Agency use of the Internet for official business is growing at a phenomenal pace, and more users are conducting business and exchanging documents via Internet e-mail.

Government agencies that use electronic mail have an obligation to make employees aware that e-mail messages, like paper records, must be retained and destroyed according to established records management procedures as set forth by Arkansas and federal law. Agencies should set up or modify e-mail systems to facilitate electronic records management. Procedures and system configurations will vary according to the agency's needs and the particular hardware and software in place.

In order to specifically address records oriented email guidelines, this document will not address policies that are focused on “appropriate use.” Appropriate use email policy is typically concerned with the proper uses of email, employee expectations of privacy for their email, employer ownership of email, email etiquette, copyright issues, and security. While that type of e-mail use policy certainly is beneficial, it fails to address significant records management issues associated with the record and/or non-record status of email, proper filing protocols, and strategies for preservation.

Scope and Intent of the E-Mail Guidelines

These e-mail guidelines apply to Arkansas state agencies. Other governmental entities may also wish to follow these guidelines as appropriate. These guidelines will assist agencies in the management of electronic mail (e-mail) messages as public records within Arkansas state government. The intent of these guidelines is to provide and explain requirements, guidelines and best practices for electronic mail (e-mail) messages that meet the criteria for records as defined by the Arkansas Code.

The purpose of the guidelines is to ensure that Arkansas government's electronic mail systems support the department's business functions to their full capability. The guidelines are not intended to discourage the use of e-mail to conduct state business, but rather to establish a framework for its proper use as a communications tool. Consistency, predictability, and reliability in the manner in which the e-mail system is used and in which public records are maintained within state agencies are the primary focuses of this policy.

The guidelines have a two-fold purpose. First, they are intended to enable Arkansas state employees to comply in their use of the agencies' e-mail systems with Arkansas Public Records Law (Arkansas Code 25-19-105; examination and copying of public records and 13-4-104; title to records). Secondly, the guidelines promote best practices and suggestions that facilitate the effective capture, management, and retention of electronic messages as public records.

Definitions

E-mail systems are store-and-deliver software systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local area network e-mail system that shuffles messages to users within an agency or office; to a wide area network e-mail system that carries messages to various users in various physical locations; to Internet e-mail that allows users to send and receive messages from other Internet users around the world.

E-mail messages are electronic documents created and sent or received by a computer system. This definition applies equally to the content of the communication, the transactional information, and any attachment associated with such communication. Thus, e-mail messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

Transitory E-mail messages: This record series consists of those records that are created primarily for the communication of information, as opposed to communications designed for the relaying of knowledge and have administrative value. Transitory messages do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt. The informal tone of transitory messages might be compared to a communication that might take place during a telephone conversation or conversation in an office hallway. Transitory messages are messages that would include, but not be limited to: e-mail messages with short-lived or no administrative value, voice mail, self-sticking notes, and telephone messages.

Access and Confidentiality

Arkansas Code 13-4-103 defines a record as:

> *... all papers, correspondence, memoranda, accounts, reports, maps, plans, photographs, sound recordings, or other documents, regardless of physical form, including records produced by or for use with electronic, micrographic, or mechanical data processing devices, and which have been or shall be created or received by any agency or its lawful*

> *successor, or official thereof in the exercise of his or her office or in the conduct of any business or function pursued in accordance with law.*

Whether the e-mail serves to document the organization, functions, policies, decisions, procedures, operations or other activities is the deciding factor as to its status as a record. This is true of any communication, whether electronic or paper.

E-mail messages that meet the criteria of the definition of a record may be considered public records and must be available to the public. A record must meet the definition of a public record as defined in the Arkansas Freedom of Information Act:

> *"Public records" means writings, recorded sounds, films, tapes, electronic or computer-based information, or data compilations in any form medium, required by law to be kept or otherwise kept, and which constitute a record of the performance or lack of performance of official functions which are or should be carried out by a public official or employee, a governmental agency, or any other agency wholly or partially supported by public funds or expending public funds. All records maintained in public offices or by public employees within the scope of their employment shall be presumed to be public records. "Public records" does not mean software acquired by purchase, lease, or license.*

As with any format, an e-mail message is considered a public record (unless it falls under one of the exceptions listed in Section 25-19-105b). These records must be maintained through the appropriate retention period and made accessible to the public upon request.

Throughout the Arkansas statutes, there exist numerous specific exemptions to the access and inspection requirements of the public records law. For this reason, users will be responsible for assuring that any public records that are exempt from access or inspection by statute will be safeguarded in a manner consistent with the practices normally provided for public records in a paper format.

Retention of Electronic Mail

E-mail messages that meet the definition of a public record in the Arkansas Freedom of Information Act (AR Code 25-19-103) are official records and must be scheduled, retained and disposed of as such. Transmitting such records electronically does not alter the obligation to retain these records, nor does it alter corresponding retention periods. Each state agency will need to determine its own e-mail retention requirements that follow state and federal record retention requirements. The content of e-mail messages may vary considerably, and therefore, this content must be evaluated to determine the length of time the message must be retained.

Each state agency will comply to applicable standards and policies concerning electronic records retention established by the Executive CIO in collaboration with the CIO Council.

> *The Executive CIO shall oversee the development of legislation and rules and regulations affecting electronic records management and retention, privacy, security, and related issues (AR Act 1042).*

Arkansas Act 905 (The Uniform Electronic Transactions Act)

> *Section 17:<u>Creation and Retention of Electronic Records and Conversion of written records by governmental agencies.</u> (a) Each governmental agency of this State shall determine whether, and the extent to which, it will create and retain electronic records and convert written records to electronic records. (b) Each state agency shall comply with applicable standards and policies adopted or established by the Executive Chief Information Officer, in collaboration with the Chief Information Officer Council to determine whether and the extent to which it will retain and convert written records to electronic records.*

<u>Non-Record Materials</u>

E-mail messages not meeting the criteria of the Arkansas Code definition of a record may be deleted at any time, unless it becomes part of some official record as a result of special circumstances. Employees should be encouraged to delete this type of correspondence as soon as possible. Deletion will free valuable disk space and allow the user easier access to needed files by avoiding unnecessary clutter within individual e-mail accounts. These types of messages may include:

- <u>Personal Correspondence</u>: Any e-mail not received or created in the course of state business, may be deleted immediately, since it is not an official record: the "Let's do lunch" (not a State business lunch) or "Can I catch a ride home" type of note. Other examples would include any personal messages not conveying state business.
- <u>Transient correspondence</u>: E-mail that is determined to have insufficient value to warrant its preservation may be deleted upon receipt. Examples are listserve messages, announcements regarding departmental bake sales and other agency memos without legal, administrative, fiscal or historical value.
- <u>Non-state publications:</u> Publications, promotional material from vendors, and similar materials that are "publicly available" to anyone, are not official records unless specifically incorporated into other official records. In the electronic world, this includes listserv messages (other than those you post in your official capacity), unsolicited promotional material ("spam"), files copied or downloaded from Internet sites, etc. These items may be immediately deleted, or maintained in a "Non-Record" mailbox and deleted later, just as you might trash an unwanted publication or promotional flyer. However, for example, if you justify the purchase of a particular filing system by incorporating the reviews you saved from a listserve in your proposal to your supervisor, those listserve messages become official records and must be retained in accordance with the retention schedule for purchasing proposals.

Official Records: Retain As Required

1. Transient Retention: Much of the communication via e-mail has a very limited administrative value and is deemed transient. For instance, an e-mail message notifying employees of an upcoming meeting would only have value until the meeting has been attended or the employee receiving the message has marked the date and time in his/her calendar. The user may delete these types of e-mail messages immediately after they have served their intended purpose. Other e-mail messages that have limited administrative value would include: telephone messages, drafts and other limited documents that serve to convey information of temporary importance in lieu of oral communication. It would only be necessary to retain these until no longer of administrative value.

2. Intermediate Retention: E-mail messages that have more significant administrative, legal and/or fiscal value but are not scheduled as transient or permanent should be categorized under the appropriate record series. These may include (but are not limited to):
   - General Correspondence: Includes internal correspondence (letters, memos); also, correspondence from various individuals, companies, and organizations requesting information pertaining to agency and legal interpretations and other miscellaneous inquiries. This correspondence is informative; it does not attempt to influence agency policy.
   - Routine Correspondence: Referral letters, requests for routine information or publications provided to the public by agency, which are answered by standard form letters.
   - Monthly and Weekly Reports: Document status of on-going projects and issues; advise supervisors of various events and issues.
   - Minutes of Agency Staff Meetings: Minutes and supporting records documenting internal policy decisions.
3. Permanent Retention: E-mail messages having significant administrative, legal and/or fiscal value and are scheduled as permanent should be categorized under the appropriate record series. These may include (but are not limited to):
   - Executive Correspondence: Correspondence of the head of an agency dealing with significant aspects of the administration of their offices. Correspondence includes information concerning agency policies, program, fiscal and personnel matters.
   - Departmental Policies and Procedures: Includes published reports, unpublished substantive reports and policy studies.
   - Reflect official actions taken.
   - Convey statements of official policy or rationale for official decisions.

4. Storing Email

Many computer systems have storage limitations, so that only 60 to 90 days of messages may be stored before operational problems are experienced. E-mail records that must be maintained in electronic format past that time can be downloaded to some other magnetic storage medium, such as hard disk, tape, diskette or optical disks. The retention period for the particular series is the best indicator of which storage media to choose. E-mail that must be retained longer than two years is best retained on magnetic tape.

Agencies that do not have the technical capability to maintain e-mail records for the full retention period in an electronic format should create a hard copy printout of their e-mail records. Agencies with computers capable of maintaining e-mail records in an electronic format for the required retention may also decide that current agency use is best served by printing e-mail records to paper.

Records managers should be aware that federal court decisions in the case of Armstrong v. the Executive Office of the President has raised questions about the adequacy of using paper printouts of e-mail as the official record. The court ruled that in the particular situation involving e-mail created by the Reagan and Bush White House on the PROFS system, the paper printout was not adequate for preserving e-mail records because fundamental pieces of information were omitted on the printout that were an integral part of the electronic records, such as the identity of the sender and/or recipient and the time of receipt. If a hard copy printout of e-mail is to be preserved as the official record, it is essential that procedures be implemented for routinely printing e-mail records, including all transmission and receipt data in the system, and filing the printouts in the normal course of business.

In order for an e-mail message to be considered a complete record, it is vital that the so-called message header, which contains all the routing information, be captured and preserved along with the message content itself. Typically, the following header information is captured and permanently recorded (in an unalterable state) along with the message:

- The Sender's Email name and address
- The recipient's Email name and address
- Names/addresses of any additional recipients
- Message Subject, as declared by sender
- Date/time of transmission and receipt

Copy of Record

Note that in most cases where e-mail communication is between a sender and a recipient, it is a generally accepted practice that the sender's copy is designated as the copy of record. In other words, it is the sender's copy to which any retention requirements should apply. For example, an intra-agency memo: a memo is sent via e-mail from the DIS Personnel Office to all DIS employees. The copy of record would be the copy in the DIS Personnel Office. All other copies are merely "duplicates" and can be disposed of at will. Cases where this principle does not apply include e-mail received from other agencies or from the public.

System Design Issues

Several issues should be addressed when developing an e-mail retention program. E-mail systems in different agencies have a wide range of capabilities and characteristics. In order to determine what will ensure the most accurate, complete, and practical method of managing records transmitted by e-mail, agencies need to develop procedures that fit their specific situations. Understanding the capabilities of an agency's e-mail system is a prerequisite in determining how the records will be identified, organized and stored. An agency's LAN administrator is the best reference for understanding agency e-mail software and can suggest possible options for e-mail retention.

When addressing e-mail retention issues, keep in mind that information systems managers routinely backup servers, and the backup media is recycled on a timetable. It is important not to rely on this backup exclusively for e-mail messages, or to store non-transitory e-mail messages (e-mail with administrative value) on a local drive that is not routinely backed up. If non-transitory e-mail messages are to be filed electronically, information systems managers should be consulted and appropriate storage locations should be designated and users should be educated on classification and filing procedures so that the information will not be lost.

Subject Lines

Fill in the subject line on your e-mail both to help your recipient identify and file messages, and to help you file your OUT box messages that must be retained for some period. Subject lines should be as descriptive as possible.

The following are some examples of poor and good subject lines for the same message:

Poor or confusing subject lines	Better, descriptive subject lines
"helpful info"	"contact info"
"report"	"quarterly '01 financial report"
"minutes"	"March '01 board minutes"
"important"	"revised admin. Procedures"
"today?"	"lunch plans today?"
"news"	"new agency head appointed"

Responsibility

Roles and responsibilities of agency personnel should be clearly defined. Employees must understand and carry out their roles in records management and agencies must ensure compliance with agency procedures, Arkansas law, and possibly federal law. Unauthorized users should not be able to access, modify, destroy or distribute records.

Agency administrators, individual agency employees, records managers, information technology (IT) managers and server administrators share responsibility for managing electronic records. Agencies should clearly identify the roles of each, adopt procedures, train staff and monitor compliance on a regular basis. The creator or recipient should make decisions regarding messages. The agency should take appropriate measures to preserve data integrity, confidentiality and physically secure e-mail records.

Part III: Electronic Imaging Guidelines

Introduction

Government records, regardless of their format, are subject to the records preservation laws of Arkansas. Agency officials are responsible for managing records in ways that insure accessibility under the Arkansas Freedom of Information Act and other state statutes with regard to open records. In this effort, many agencies are implementing electronic document imaging systems to enable increased accessibility and distribution of information.

The electronic imaging guidelines are for Arkansas State and local agencies that choose to implement an electronic imaging system. The guidelines are designed to identify critical issues for agency officials to consider in designing, selecting, implementing, and operating digital imaging technologies. The guidelines provide recommendations and are not intended to serve as a rigid set of requirements. However, the degree to which they are incorporated into system design will greatly effect the long-term accessibility of the electronic records involved. These issues are especially important for systems used for mission critical records or for long term archival records.

Digital imaging is defined as the ability to capture, store, retrieve, display, process, and communicate or disseminate records electronically using a variety of hardware and software components. Electronic document management and imaging systems are computer-based systems that store digitally encoded document images. These systems are deployed as an alternative to paper based document systems and provide image retrieval and distribution on demand. An electronic document imaging system should be deployed, as a tool to enable increased accessibility and distribution of information and to reduce the time required to perform those functions.

All references to "document" and document management systems in these guidelines should be considered as references to "Official State Records" and the management of those records.

Scanning Technologies

Scanning is the technique used to capture images from a human eye readable format (documents, microform, photographic prints, posters, magazine pages and similar sources) for computer editing, display and storage. The process of scanning documents is also referred to as imaging.

Scanners usually attach to a computer using a hardware interface and come in hand-held, higher speed multiple document feed-in, and single sheet flatbed types. Scanners are usually designed to support black-and-white only and/or color documents and various document sizes. Newer technologies combine the functions of high speed printing, copying and scanning. These devices can participate as managed units on a computer network.

Very (high-resolution) scanners are used for scanning of documents that require a high level of fine detail (photos, maps, etc.), but lower-resolution scanners are typically adequate for capturing documents for document management systems.

Scanners are usually supported with scanning software and hardware that allows for quality improvement of a captured image. A quality assurance (QA) process used to guarantee the quality of documents and information captured during the scanning process is the single most important activity performed to assure the integrity of a document management system.

Project Planning

Before committing to a document imaging application, public agencies should perform a feasibility study to ensure that a document imaging system is appropriate for its information management needs. One of the first steps would be to conduct a records and workflow analysis to determine and document existing and planned agency information needs. The examination of existing workflow patterns and records is the crucial first step in determining the need for a digital imaging system. A records analysis assesses existing operations to determine what records are best suited for digital imaging applications. A workflow analysis assesses the processes of records creation, access, and retrieval to determine areas where reengineering can improve operational efficiency. This reorganization of work processes may be simple or extensive in approach. Implementing a digital imaging system significantly impacts the current work processes because personnel create, retrieve, use, and store documents in a different way.

The following topics need to be analyzed and evaluated before implementing a well-planned Electronic Document Management System:

- Workflow evaluation
  - What documents are used in the course of performing each business process?
  - What is the average volume for each type of document per year?
  - Are there seasonal factors or peak load times to consider per business process?
- A complete inventory of existing records
- Data needs assessment
- Network support
- Cost/benefit analysis
- Projected growth
- Retention and legal requirements

Open System Architecture

Require open systems architecture for digital imaging applications or require vendors to provide a bridge to systems with non-proprietary configurations. Although the term open systems architecture is defined in various ways, agency officials should follow a system design approach that permits future component upgrades with minimal degradation of system functions. This open system architecture allows the system to be upgraded over time without a significant risk of records loss. It also supports the importing and exporting of digital images to and from other sources. One key factor in achieving open systems architecture is the adoption of non-proprietary standards. The flexibility of an open systems architecture helps enable long-term records to be accessed and transferred from one hardware or software platform to another.

Maintenance of Records For Electronic Management Systems

State and local government officials may maintain public records in an electronic imaging system. Once this is accomplished there is a need to dispose of the originals provided they:

1. Maintain security copies of the disks, tapes, and indexes in off-site storage.
2. Migrate and convert both the working and security copies of the disks, tapes, and indexes if the systems are upgraded or changed in a way that prevents access to the contents of the old system.
3. Sample both the working and security copies of the disks and indexes at least once a year to make certain the data is readable and recopy to new media immediately if any loss of information is detected.

Arkansas Code Ann. 16-46-101 permits government agencies to destroy original records that have reproduced in a "durable medium," unless law requires preservation of the original.

Storage Solutions

Attempt to employ recording media that is not rewritable, especially when data longevity or records integrity is a primary concern. The storage capacity of optical disks versus paper is a primary advantage to the use of electronic document management systems. However, optical disks are not the only option. Other storage solutions that can be used with e-document management systems include output to microfiche or microfilm, digital tape, and magnetic disks. The selection of a storage media may depend on budget considerations for the agency.

Use of Records Management Application (RMA) Software

Agencies may use Records Management Application (RMA) software to manage records in digital form. RMA software categorizes and locates records and identifies records that are due for disposition. RMA software also stores, retrieves, and disposes of the electronic records that are stored in its repository. The U.S. Department of Defense has issued, "Design Criteria Standard for Electronic Records Management Software Applications," that can serve agencies in their selection process.

General Guidelines

To maintain effective operation and to be able to retrieve data as operating environments change over time, it is necessary to keep full documentation of:

- Hardware and software, including brand names, version numbers and dates of installation, upgrades, replacements, and conversions.
- Data structure and content, including the file layout.
- Operating procedures, including: methods for scanning or entering data; revising, updating, or expunging records; indexing, backing up disks, tapes, microfilm, etc.; testing the readability of records; applying safeguards to prevent tampering and unauthorized access to protected

information; and carrying out the disposition of original records. In addition, to provide audit trails, it is necessary to document procedures for logging and tracking.

Recommended System Criteria

Open system: Agencies shall require open systems architecture for electronic imaging applications or require vendors to provide a bridge to systems with non-propriety configurations (integration across platforms).

Scanning resolution: When determining document-scanning resolution, agencies shall consider data storage requirements, document scanning throughput rates, and the accurate reproduction of the image. Vendor claims shall be validated using a sampling of the agency's documents. Calibration and maintenance of the scanners should meet the manufacturers' recommended schedule.

The following minimum resolution readings are for black and white documents. Standard text office documents. A minimum resolution of 200 dots per in (dpi) is recommended. Drawings, maps and plans. A minimum resolution of 300 dots per inch is recommended. Deteriorating documents or documents with fine detail. A minimum resolution of 600 dots per inch (dpi) is recommended.

Indexing: Agencies should use an indexing database that provides for efficient retrieval, ease of use, and up-to-date information about the digital images stored in the system. The indexing database shall be selected after an analysis of agency operations and user needs.

Staffing: The agency assign a permanent staff member as system administrator and require the vendor to provide a project director during the installation and training periods. The assignment of a qualified staff member, preferably with systems administration experience, is critical to the effective implementation and maintenance of a digital imaging system. The systems administrator should be responsible for overall project management, and the development and maintenance of written system documentation, which describes the requirements, capabilities, limitations, design, operation, and maintenance of the digital imaging system.

Documentation: The agency establish operational practices and provide technical and administrative documentation to ensure the future usability of the system, continued access to long-term records, and a sound foundation for assuring the system's legal integrity.

Quality control: It is advised that the agency perform a weekly scanning quality test.

Media handling, backup, and storage:

Labeling: Disks, tapes, and other storage containers labeled with particular care since it is impossible to determine content merely by looking at a disk or tape. Labeling is critical when the disk and its index are stored on different media.

Security copies: Security copies marked with appropriate external labels that identify the government entity, system and software used, and any access restrictions.

Documentation: Maintain specific, detailed documentation of the contents and the system specifications needed to access each media type.

Backup: Implement backup procedures to create security copies of electronic files and their related index records. System component reliability is critical to system success. Prolonged or repetitive downtime can seriously affect office operations. Creating a duplicate copy of records in another format or another system is an effective method of ensuring access to long-term information. Backup copies also support system integrity and legal admissibility requirements. The agency may select the backup storage media (optical, magnetic, or microform) that best meets the office's records requirements. Security copies of the records should be stored in an offsite, environmentally controlled location.

Appropriate Formats For Accessibility

When implementing document management solutions, it is important to produce scanned files that are accessible for individuals who are blind or visually impaired. Most scanning software provides options as to what type of file format the scanned document is saved. The option is usually given to save as some type of text document (i.e. ASCII text, RTF, HTML, XML, commonly used word processing files such as Word or PDF). HTML and XML requires a lot more disk space due to html formatting. If saved in one of these text formats, it is accessible for visually impaired individuals using adaptive technologies.

If the scanned document is saved as an image then it is totally inaccessible to a person using adaptive technology. Any type of graphic format such as TIF, PCX, BMP, GIF, JPG or any other type of image-based file will not be accessible for the visually impaired. If the scanning conversion software does not allow for saving documents in anything other than an image, then it is probably in violation of state and federal law and should not be used.

Items such as photographs, graphs, diagrams, or any other type of visually presented material are not capable of being made accessible. If a document to be scanned had such material on the page then the graphical portion could be scanned in as an image but the text portions would need to be saved as some type of accessible text format.

Arkansas' Enterprise Documentation Organization & Capture System

The Arkansas Department of Information Systems (DIS) is offering an enterprise electronic document management solution for Arkansas government entities. The enterprise document management solution establishes a state environment for agencies to electronically store, index & manage all forms of documents (scanned images, MS Word and Excel files, drawings, etc). The benefit of utilizing the state enterprise solution is it insures interoperability of electronic document and electronic records management systems implemented by state agencies

Identitech was the successful bidder for the state-wide imaging solution. Identitech's software product name is FYI. FYI is an open architecture product, which supports a wide variety of third-party hardware and software environments.

Identitech's Highlights

- Quickly index, image, annotate & store documents
- Provides search criteria & quick retrieval capabilities - full text search available
- Provides system growth without system replacement
- Can scan both sides of a document simultaneously
- Can not alter the original document - as notations made, versions created
- Can apply multiple indices to a document
  - Bar codes, OCR/ICR allowed

Key selection criteria

The Arkansas Department of Information Systems (DIS) utilized the following criteria in selecting the enterprise imaging solution.

- Quickly image, index, annotate and store documents
- A user friendly windows type interface for staff and others to use
- Provide training sessions
- Provide search criteria & quick retrieval capabilities
- Full text search capability
- Provide security and document integrity
- Provide system growth without system replacement
- Can scan both sides of a document simultaneously
- Can not alter the original document – as notations made, versions created
- Can apply multiple indices to a document (bar codes, OCR/ICR allowed)
- Provide for document check in / check out capabilities
- Provide comprehensive backup & recovery capabilities
- Organizes images into folders indexed by claimant, employer, or other identifying characteristics with multiple indices available
- Documents can be viewed concurrently by multiple users in multiple locations
- Able to share documents via fax or e-mail
- Provides on-line help
- Capable of variable resolution
- Able to accommodate multiple sized paper
- Able to support TIFF, GIF, JPG, PDF, JPEG, and MPEG image formats
- Provides zoom in / zoom out capabilities
- Is AASIS (SAP) compatible
- Able to store Word, Excel, diagrams, charts, etc. as a part of a folder

Current Status

- Identitech's product, FYI, is in place & functioning
- Security & backup processes are in place

- Employment Security Dept is beginning to initiate their pilot project for Unemployment Insurance processing
- Arkansas Dept of Education is piloting their Professional Licensure process

Training Available

DIS will provide the following training to agencies that implement the enterprise document imaging solution:

- Preparing your Agency for Electronic Document & Workflow Management
  - Provide facilitator for business process analysis & analyze selected process
- System Administrator's Training
  - Introduction / orientation to FYI and it's components
  - Logging in and maintaining your users and their profiles of what they can / can not do
  - Creating workgroups and work flows
  - Defining folders, documents, and their indices
  - Adding electronic annotations to documents
  - Producing reports
  - Troubleshooting tips
  - Hints for effective use
- End User's Training
  - Introduction / orientation to FYI and it's components
  - Screen components
  - Screen types
  - Logging into FYI
  - Introduction to the Main Menu

Internal and external controlled security

- Currently: no access via the Internet allowed at this time
- Access through the State Trusted Network Access
- Predefined user profiles determine access levels
- Web browser can be used

For more information on the State Enterprise Imaging System, contact Danna Erwin, DIS Project Manager at danna.erwin@mail.state.ar.us

Appendix I: Web-Available Resources

Association of Records Managers and Administrators International (ARMA)
ARMA Email Guideline Development Task Force

Association of Records Managers and Administrators Resources

Association for Information and Image Management

Center for Technology in Government, University at Albany, Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation

"Design Criteria Standard for Electronic Records Management Software Applications," as issued by the U.S. Department of Defense.

National Archives and Records Administration (NARA) Fast Track Guidance Development Project (To identify currently available "best practices" and provide guidance quickly on electronic records issues that urgently confront Federal record keepers)

Kansas Electronic Records Guideline: http://www.kshs.org/archives/ermguide.htm#intro

New York State Office for Technology: Electronic Signature and Records Act (ESRA) Guidelines: E-Signature Performance, E-Signature Security, E-Records
http://www.oft.state.ny.us/esra/Guidelines_files/index.htm

Utah State Archives and Records Service:
http://www.archives.state.ut.us/recmanag/electronic.htm

Appendix II: Glossary

Accessibility - is the attribute of records or information being available for appropriate use over time. For e-records accessibility includes having the technical means and metadata (data describing how, when, and by whom an e-record was created, and how it is formatted) to access, use, and understand the records.

Authenticity - Refers to the methods used to verify the source or origin of an e-record. Authenticity is closely related to the concept of ***integrity***.

Custodian - With respect to personal information, it means the person having administrative control of that information (record), or his or her designee. "Custodian" does not mean a person who holds public records solely for the purposes of storage, safekeeping, or data processing for others.

Document Imaging - The online storage, retrieval and management of electronic images of documents. The main method of capturing images is by scanning paper documents.

Electronic Document Management and Imaging Systems - Computer-based systems that store digitally encoded document images. These systems are deployed as an alternative to paper based document systems and provide image retrieval and distribution on demand. An Electronic Document Imaging System should be deployed, as a tool to enable increased accessibility and distribution of information and to reduce the time required to perform those functions.

Electronic imaging system - A computer-based system that stores digitally encoded document images. These systems provide image retrieval and distribution on demand. They are an alternative to paper or microfilm record systems.

Electronic record – any record created, stored, sent or received in a non-tangible form, including by or relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. Source: Adapted from UETA, Sections 102 (5) and 102(7).

Electronic record-keeping system - An electronic system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

E-mail systems – store-and-deliver software systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local area network e-mail system that shuffles messages to users within an agency or office; to a wide area network e-mail system that carries messages to various users in various physical locations; to Internet e-mail that allows users to send and receive messages from other Internet users around the world.

E-mail messages - electronic documents created and sent or received by a computer system. This definition applies equally to the content of the communication, the transactional information, and any attachment associated with such communication. Thus, e-mail messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

Encryption - The process of enciphering or encoding data so that it is inaccessible to unauthorized users.

Integrity - is the attribute that the record's contents have not been changed, deleted or otherwise altered. In addition, integrity addresses the accuracy and timeliness of the contents of a record. Both authenticity and integrity are derived from the legal arena and have a strong bearing on the legal admissibility of records.

Open System - A system that implements sufficient open standards for interfaces, services, and supporting formats to enable properly engineered components to be utilized across a wide range of systems with minimal changes, to interoperate with other components on local and remote systems, and to interact with users in a style that facilitates portability. An open system is characterized by the following:

- well defined, widely used, preferably non-proprietary interfaces/protocols;
- use of standards which are developed/adopted by recognized standards bodies or the commercial market place;
- definition of all aspects of system interfaces to facilitate new or additional systems capabilities for a wide range of applications; and
- explicit provision for expansion or upgrading through the incorporation of additional or higher performance elements with minimal impact on the system.

Public Records - means writings, recorded sounds, films, tapes, electronic or computer-based information, or data compilations in any form medium, required by law to be kept or otherwise kept, and which constitute a record of the performance or lack of performance of official functions which are or should be carried out by a public official or employee, a governmental agency, or any other agency wholly or partially supported by public funds or expending public funds. All records maintained in public offices or by public employees within the scope of their employment shall be presumed to be public records.

Transitory E-mail messages - consists of those records that are created primarily for the communication of information, as opposed to communications designed for the relaying of knowledge and have administrative value. Transitory messages do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt. The informal tone of transitory messages might be compared to a communication that might take place during a telephone conversation or conversation in an office hallway. Transitory messages are messages that would include, but not be limited to: e-mail messages with short-lived or no administrative value, voice mail, self-sticking notes, and telephone messages.

Security - refers to the protection of information assets, including both physical and technical controls over access to information. Security has technical, physical, and procedural components.

State Data - is the body of data that has been collected by various means and must be retained by state agencies in order to accomplish legislated and otherwise assigned responsibilities. All state data is owned by the residents of the state but is managed, maintained, and protected by state agency custodians.

Appendix III. Acknowledgements – Arkansas Information Architecture Working Group Members

Andy Adams:	Legislative Audit
Randy Apon:	University of Arkansas
Claire Bailey:	Department of Information Systems
Harold Bailey:	Department of Information Systems
Glen Balmat:	Department of Economic Development
Tom Bohannan:	Employment Security Division
Mark Barton:	Rich Mountain Community College
Fred Borum:	Cossatot Technical College
Suzanne Brabston	Department of Information Systems
Judy Brummett:	Development Finance Authority
Chad Calhoun:	Board of Nursing
Lee Clark:	Department of Health
Steve Collins:	University of Arkansas Community College at Batesville
Dan Delaughter:	Department of Parks and Tourism
Chad Douglas:	Department of Information Systems
Beatrice Ekworomadu:	Department of Parks and Tourism
Dan Frith:	Department of Information Systems
Jim Franquemont:	Department of Information Systems
Janet Girard:	Information Network of Arkansas
Tenita Gragg:	SEARK College
Melinda Green:	Insurance Department
Harold Harvey:	Department of Information Systems
Sally Hawkes:	State Library
Mary Henthorn:	Department of Information Systems
Rick Jenkins:	Southeast Arkansas College
Jim Kane:	Information Network of Arkansas
Britton Kerr:	Insurance Division
Tom Hart:	University of Arkansas Medical School
Diana Hopper:	Department of Information Systems
Laura Johnson:	Southern Arkansas University Technical College (Camden)
Keith Leathers:	Department of Human Services
Ron Lester:	Department of Finance Administration
Evelyn Looper:	Department of Information Systems
Drew Mashburn:	Department of Information Systems
Tracy Morgan	Rehab Services
Paul Nations	Department of Higher Education
Earle Norton:	Legislative Audit
Letha Osborne:	Crime Information Center
Kym Patterson:	Department of Information Systems
Jerry Perkins:	Department of Health
Kristy Pryor:	Parks and Tourism
Randy Putt:	University of Arkansas
Betti Rippentrop:	Department of Finance and Administration
Mickey Roberts:	Crime Information Center
Robert Smothers:	DCSIM
Jerry Spratt:	Legislative Audit
Patrick Stair:	Department of Environmental Quality
Paula Swaim	Department of Information Systems
Scott Utley:	Department of Information Systems
Peggy Wakefield:	Department of Higher Education
Jim Wallace:	Great Rivers Technical College
Oren Wright:	Department of Human Services