MDAH Local Government Records Office

EMAIL MANAGEMENT GUIDELINES

FOR

COUNTIES AND MUNICIPALITIES

1. Purpose

The purpose of these guidelines is to ensure that the electronic mail records of county and municipal government officials and employees are retained securely for as long as required by law.

2. Authority

These guidelines are issued by the Mississippi Department of Archives and History (MDAH) under authority granted under *Mississippi Code Annotated* (*MCA*) §§25-59-1 to 25-59-31, the Mississippi Archives and Records Management Law. The law designates MDAH as the archival and records management agency of the state. The powers and duties of the MDAH Local Government Records Office are specified in *MCA* §39-5-9.

3. Email as Public Records

Work-related email messages and attachments are public records under Mississippi law. Therefore, they must be managed the same way that other public records, whether paper or electronic, are managed.

MCA §25-59-3 defines "public records" as "**all documents**, papers, letters, maps, books, tapes, photographs, films, sound recordings or other materials **regardless of physical form** or characteristics **made or received** pursuant to law or ordinance or in connection with the **transaction of official business** by any agency or by any appointed or elected official." *[emphasis added]*

These guidelines apply to any email message that meets this definition regardless of the device or account used to create it, including personal/home email accounts, mobile computing devices such as smart phones and personal digital assistants (PDAs), and social networking websites and services.

There are many reasons to manage email records, including:

- Email has become integral to the operation of government.

- Email can have the same potential evidentiary value as any other record documenting the transaction of public business.
- Email records are subject to the same legal requirements regarding access as other public records, and requests for email records must be honored in the same manner as other records.
- Email records must remain accessible during their entire retention period and should be maintained in a manner that allows efficient and timely retrieval.

4. Basic Strategies

It is recommended that county and municipal governments define approved methods of official communication for employees at different levels with different responsibilities, and require employees to sign a statement agreeing to follow such email policies and procedures. It is also recommended that users of web-based mail services (e.g., AOL, Gmail, Yahoo Mail, etc.) should keep business and personal accounts separate. In general, employees should not use social networking websites such as Facebook or services such as Twitter for the transmission of official communications.

5. Records Control Schedules

A records control schedule is a set of instructions prescribing how long, where or in what form records shall be kept. Like other records, the retention and management of an email message is derived from its content. There is no single "one size fits all" retention schedule for email.

Records control schedules for Mississippi counties and municipalities are drafted by the MDAH Local Government Records Office and approved by the Local Government Records Committee. Once approved, the schedules carry the full force of law. Approved records control schedules may be viewed at http://www.mdah.ms.gov/new/government-2/records-management/local-government-records/record-retention-schedules/. Each office should determine the schedules relevant to the types of email it most frequently sends and receives.

6. "Record Copy" and Duplicates

The "office of record" is the unit responsible for holding the authoritative copy of an email message. For example, if the Human Resources office emails a job announcement to all staff, that office would retain the sender's copy for legal, business, and historical purposes. The copy received by other staff is for informational purposes and can be deleted when no longer useful. To determine who has the "record copy," an employee or office that is responsible for the paper version would be responsible for filing and maintaining the electronic version as well.

7. Determining How Long to Keep Email Records

The value of an email message is based on its content and function, and is often related to the position and duties of the person sending or receiving the message. Therefore, the length of time that an individual's email messages need to be retained will vary according to these factors. Generally, email messages fall within three broad categories:

a. Public records of significant value that must be retained long-term or permanently in accordance with a records control schedule.

Example: Executive correspondence of a mayor or other elected official has historical value because of the person's position and duties, and should be maintained permanently.

b. Public records of temporary value that may be disposed following a retention period defined by a records control schedule.

Example: Messages to and from the purchasing office are more likely to be related to the purchase of equipment and supplies, so most messages would fall under records control schedules for financial and purchasing records.

c. Communications that are not public records, such as transitory communications.

Transitory Communications are casual and routine messages that do not fall under the umbrella of "public records" as defined in MCA §25-59-3. Examples include:

- *Personal emails not related to work*
- *Spam or unsolicited advertisements*
- *Incoming electronic mailing list messages*
- *Non-policy announcements*
- *Thank yous*
- *Attachments to messages that are identical to records that are stored and managed outside the email system pursuant to approved records control schedules*
- *Out-of-office automatic replies*
- *Published materials*
- *Replies to routine questions (hours, address, directions, etc.)*

Public employees and officials sending and receiving such emails may delete them when no longer useful.

8. Options for Managing Email Records in Accordance With Records Control Schedules

There is no single method for ensuring compliance with legal records retention requirements. Any method chosen must be adopted system-wide and incorporated into written policy for uniformity across all departments and employees. There are a number of acceptable ways, including:

a. Treat all email records as correspondence: apply the appropriate records control schedule(s), folder by year, and separate the permanent from the non-permanent records.

b. Create a file plan based on scheduled records series: organize your email records in a file plan that aligns them with the pertinent schedules.
When implementing this structure, the user can create subfolders as needed, each linked to a series with a scheduled retention period. Creating a subfolder for each year (calendar or fiscal) helps the user dispose of records in a timely manner. For example, if the schedule calls for the series to be held 3 years then disposed, filing by year will prove beneficial. Example:

jsmith@mdah.ms.gov
Inbox
Sent
Trash
Administrative Files
    2007
    2008
    2008
    2010
Procurement Files
    2007
    2008
    2009
    2010
Routine Working Files
    2007
    2008
    2009
    2010

c. Group non-permanent records by functional category (administrative, financial, etc.): simplify retention and disposition by filing multiple scheduled series together, foldering by year, and applying the longest retention period to all, **OR** group by functional category, folder by retention period (keep 5 years, keep 3 years, etc.) and subfolder by year.

d. Print and file email records as part of a paper recordkeeping system. Those who choose this method should be aware that an authentic, complete email record consists of the email message together with its attachments and transmission data. It is important to print the attachments and message source information along with the message itself. Each email client has a slightly different way to access and print the message source information. If the email client prevents access to the full source information, print the message with its full header.

9. Electronic Storage and Maintenance of Email Records

Approaches to storing, maintaining, and accessing email records electronically are highly dependent on levels of financial resources and IT support. Proper and regular backup procedures must be in place regardless of the method used.

Minimum requirement:

a. Storing email records within an electronic mail system. Due to mailbox size limitations in most organizations, this should not be viewed as a permanent solution. Additionally, if this method is used, closed email accounts must not be deleted until it has been verified that all public records have been transferred to another recordkeeping system or that any scheduled retention periods have expired and there is no pending litigation, audit, investigation, or public records request.

Other methods include but are not limited to:

b. Creating folders that are stored outside of the mailbox on a desktop or server but that can be viewed using the email client.

c. Storing and managing email records through use of an email archiving software application.

d. Storing and managing email records along with other electronic records through use of an enterprise content management (ECM) system.

Other considerations:

- Before purchasing an email archiving system, see Guidelines for Selecting Email Archiving Systems and Providers, Appendix III.
- For an email service hosted by a third party, it is the responsibility of the local government to ensure that the host is aware of legal requirements to manage email messages as public records.
- If a local government official or employee creates public records through the use of a web-based service such as Gmail, Yahoo Mail, etc. or a social networking website such as Facebook, it is that person's responsibility to ensure that messages can be saved and stored as records outside of the service, or at minimum he/she should print and file them. Users of web-based mail services should keep business and personal accounts separate.
- Any storage/maintenance method employed must ensure that electronic files with long-term retention requirements are migrated to new versions of software as necessary to guarantee continuing accessibility, and, if possible, converted to a non-proprietary file format such as XML to support long-term preservation.

10. Confidential Email

Every effort should be made to protect confidential or private information from disclosure and from losing its confidential or private status. Local governments should have policies and procedures in place to ensure that employees understand the risks involved in transmitting such information via email. They should also consider the use of an email disclaimer – a statement, usually of a legal character, that can be appended to an email message to warn that the contents are confidential. In addition to breach of confidentiality, email disclaimers can be used to address transmission of viruses, entering into contracts, negligent misstatements, and employer liability.

11. Electronic Discovery (E-Discovery)

The Mississippi Rules of Civil Procedure address the discovery of electronic data in Rule 26: General Provisions Governing Discovery. The rules may be viewed online at:

https://courts.ms.gov/newsite2/research/rules/rules.php

The Federal Rules of Civil Procedure were amended effective December 1, 2006 to recognize and accommodate the discovery of "electronically stored information," defined as information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software. The fact that the email and other electronic files of an agency or official are subject to discovery in the event of litigation reinforces the need to provide for their organization, search-ability, and legally-established retention and disposition.

12. Contact Information

Managing email depends greatly on one's particular situation – IT structure, financial resources, email client (or clients), server implementation, internet protocols, storage formats, etc. For technical questions pertaining to the management of email records, contact the MDAH Electronic Archives section at elecrecs@mdah.ms.gov.

For questions pertaining to the scheduling, retention, and disposition of county and municipal records, contact the MDAH Local Government Records Office at (601) 576-6894 or by email at locgov@mdah.ms.gov.

Comments and suggestions for revisions of these guidelines are welcome; please contact either office listed above.

Appendices

I. Definitions

II. Sample Email Management Policy for County and Municipal Governments

III. Guidelines for Selecting Email Archiving Systems and Providers

Appendix I

Definitions

Data migration – the process of transferring data between storage types, formats, or computer systems that is required when organizations or individuals change computer systems, upgrade to new systems, or when systems merge.

Electronic discovery (e-discovery) – discovery in civil litigation which deals with information in electronic format.

Electronic mail system – a computer application used to create, receive, and transmit messages and other documents.

Electronic mail message – a document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents which may be transmitted with the message.

Electronic record – a record created, generated, sent, communicated, received, or stored by electronic means (*MCA* §75-12-3).

Electronically stored information (ESI) – information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software.

Email archiving – a systematic approach to saving and protecting the data contained in email messages so it can be accessed quickly at a later date.

Email client – a computer program used to manage email. Also known as a mail user agent.

Enterprise content management (ECM) system – the technologies used by organizations to capture, manage, store, and control enterprise-wide content, including documents, images, email messages, instant messages, video, and more.

Email hosting service – an Internet hosting service that runs email servers.

Internet protocol – the method or protocol by which data is sent from one computer to another on the Internet.

Public records – all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other materials regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency or by any appointed or elected official. Books, periodicals and other published material normally found in a library are excluded from this definition (*MCA* §25-59-3).

Receipt data – information in electronic mail systems regarding date and time of receipt of a message, and/or acknowledgment of receipt or access by addressee(s).

Records control schedule – a set of instructions prescribing how long, where or in what form records shall be kept (*MCA* §25-59-3). Also known as a *records retention schedule*.

Retention period – the length of time that a record must be kept according to an approved records control schedule.

Transmission data – information in electronic mail systems regarding the identities of sender and addressee(s), and the date and time messages were sent.

XML – Extensible Markup Language, a set of rules for encoding documents in machine-readable form, used as a preservation format for email messages and other electronic files.

Appendix II

Sample Email Management Policy for County and Municipal Governments

This policy defines acceptable management and storage of email messages in *[name of entity]* as part of its records management program.

Email Messages as Public Records

Email is a means of transmission of messages or information. The content and any attachments associated with the email are considered a record if they meet the definition of "Public Records" in *Mississippi Code Annotated (MCA)* §25-59-3(b):

> "***all documents***, *papers, letters, maps, books, tapes, photographs, films, sound recordings or other materials* ***regardless of physical form*** *or characteristics* ***made or received*** *pursuant to law or ordinance or in connection with the* ***transaction of official business*** *by any agency or by any appointed or elected official. Books, periodicals and other published material normally found in a library are excluded from this definition.*"

This policy applies to any email message that meets this definition regardless of the device or account used to create it, including personal/home email accounts, mobile computing devices such as smart phones and personal digital assistants (PDAs), and social networking websites and services.

Retention and Disposition of Email Messages

Like paper records, the retention or disposition of email messages is determined by the information they contain or the purpose they serve. Since the content may vary considerably, it must be evaluated to determine the length of time the email must be retained. As with paper records, this retention period must be specified in a records control schedule, defined in *MCA* §25-59-3(h) as a "set of instructions prescribing how long, where or in what form records shall be kept." In accordance with Mississippi's Local Government Records Law (*MCA* §25-60-1), all schedules are approved by the Local Government Records Committee and once approved, a schedule carries the force and effect of law. Approved schedules are available at the website of the Mississippi Department of Archives and History (http://www.mdah.ms.gov/new/), which is responsible for the implementation of the Local Government Records Law through its Local Government Records Office.

Email records, whether maintained electronically or managed by printing and filing, must be maintained in a filing structure that identifies them as belonging to a group of records with a retention period defined by an approved records control schedule.
Records can be destroyed only according to approved records control schedules.

Per *MCA* §25-61-1 et seq. certain electronic documents, including email, are legally discoverable and accessible under the Mississippi Public Records Law. It is the policy of *[name of entity]* to

fully comply with any records request made under this section and in accordance with this policy as approved.

Non-record Email

Email messages that do not meet the definition of "Public Records" may be disposed of when no longer useful. Examples include incoming listserv/mail list messages, spam, unsolicited advertisements, invitations, thank yous, replies to routine questions, out of office replies, and attachments to email messages that are identical to records that are stored and managed outside the email system pursuant to approved records control schedules.

Responsibilities of *[name of entity]*

The *[name of entity]* will implement the necessary procedures to ensure the appropriate management and retention of email, including but not limited to the following:

- Ensure that all records are covered by and managed according to current records control schedules.
- Establish a file management plan based on the schedules, regularly creating new folders to make it easy to dispose of records as allowed by the schedules.
- Ensure that any email records that are subject to a litigation hold or e-discovery/public records request are preserved and accessible as long as required.
- Ensure that electronic files with long-term retention requirements are migrated to new versions of software as necessary to guarantee continuing accessibility, and, if possible, converted to a non-proprietary file format such as XML to support long-term preservation.
- Ensure that all employees receive training in records management as well as any specialized training needed to implement this policy.
- Define approved methods of official communication for employees at different levels with different responsibilities, and have employees sign off on a policy defining appropriate methods for their position.
- Regularly notify the *[insert name of entity's information technology office]* when the accounts of former employees can be closed.
- Ensure that all employees are aware of and implement this policy.

Exceptions

Exceptions to this policy may be granted in writing by the *[insert title of person/people]*.

Appendix III

Mississippi Department of Archives and History
Archives and Records Services Division

Guidelines for Selecting Email Archiving Systems and Providers

1. Consider your retention needs. Email records must be retained according to their content, and therefore will not all have the same retention period. For email records that meet the definition of "Public Records" in §25-59-3 of the Mississippi Code, their retention period must be based on a records retention schedule approved by either the State Records Committee or the Local Government Records Committee. Implementation of an archiving system must include planning for filing, managing, and disposing of records based on their legally approved retention periods.

2. Determine the basic approach that matches your particular capabilities, financial resources, and needs. Options include:

- Out-of-the-box hardware-based systems that are deployed and managed by in-house personnel
- Software products that are installed and managed by in-house personnel
- Services hosted/managed by a provider
- Hybrid systems using in-house personnel and an outside service provider

3. Consider systems that support all email platforms. If your office currently uses different messaging systems, or if you want the flexibility to migrate to another platform in the future, choose a system that supports all email platforms.

4. Consider your storage needs and plan for future growth. Look for a scalable system that can grow with your needs and help optimize storage costs.

5. Consider your access and searchability needs. Make sure that your system is capable of meeting your search functionality needs when you are required to respond to electronic discovery and other public records requests.

6. Consider extensibility to other systems. While your immediate concern may be email, in the future you might want to extend your system to cover other data. Take a long-term view toward the type of information you will need to archive.

7. Look for a system that is easy to learn and use, to reduce training requirements for IT personnel and other system users.

8. Consider your backup needs. When planning your system, think of your needs for redundancy, off-site storage, and data security for protection from natural disasters, equipment failure, theft, and systems disruptions.