ELECTRONIC MAIL FOR STATE AGENCIES

A Guideline of the Utah State Archives and Records Service

March 2017

PURPOSE: In light of the prevalent nature of email systems in Utah State government, and as a result of good business practices, legislation, and litigation, the ability to appropriately store, manage, and purge the email of State of Utah employees has become imperative. Email is the main method of communication in many areas of State government. It is often an official record of what has transpired. At the same time, it is used for non-official purposes such as personal messages and transitory matters. All of this information typically is stored in email systems and on backup tapes without regard to need, importance or content, kept for the same length of time, then purged, again without regard to need, importance, or content. Several problems arise from these circumstances:

1. Records of value—those needed by an agency to document its own actions or make decisions based on that information or which provide accountability to the public—are not placed where their survival can be guaranteed. Such records often have historical research value after a period of time or are needed for litigation. Emails of no value are kept, often in multiple places, and then take up server space, cause unnecessary expense in keeping them and interfere with attempts to find valuable records.

2. Email originates with a single user, though it may be sent to many recipients. In turn, it may be forwarded by original recipients to further recipients, thus creating a trail of duplicates that is difficult to manage and typically unnecessary from a records management perspective.

3. Emails that are deleted from a sent or received box by a user may continue to exist in other boxes, on servers, or elsewhere. This results in inconsistent applications of legal retention periods, complicating searches in response to open records requests or for e-discovery.

346 S Rio Grande St • Salt Lake City, Utah 84101
Telephone (801) 531-3848 • Facsimile (801) 531-3854 • ***archives.utah.gov***

4. Backup systems are not recordkeeping systems; however, they are often forced into that role. Backup systems ideally should only be used for disaster recovery.

5. Records of value, even if kept by the creator, usually are not in a centralized location accessible to others in the agency that may need the information.

The technology required to effectively manage email records is available and is quickly expanding in terms of the scope and efficiency of services offered. As State correspondence becomes more and more electronically based, the availability of such products makes it possible, and necessary, to institute a sound and comprehensive email management policy. Acknowledging that records management needs, workloads, and complexities vary widely across State government, the intent of this guideline is to establish baseline standards that ensure legal compliance but are still broad enough to provide each agency the flexibility to shape management practices to fit their unique requirements.

Email systems, and the number of devices capable of accessing them, will continue to grow in complexity, so related policies and procedures should be reviewed and updated as necessary.

DEFINITIONS

Proprietary and Non-proprietary Formats

Format refers to essential characteristics of an electronic file. Email often exists as both an electronic format and a file format. File formats are often proprietary, meaning they are controlled and readable only through the software of a single company and thus only on computers that run that software. Since proprietary files cannot be exported to any other environment, it is necessary to ensure that emails are created in, or can be converted to, non-proprietary formats.

Style Format

RFC 2822 is the international standard applied to the vast majority of emails. It defines email as consisting of a header, with routing information, and a body, which contains the message, separated by a blank line. Users may add other features to this format, such as a signature, that will be applied to each email sent. It is essential that the format of emails be preserved and that they are viewable as they were created. Some means of saving emails, such as plain text, do not preserve the original format, and thus are not ideal for the purposes of records management.

Metadata

Email records include not only the text of the message, but all of the accompanying contextual information that the email system tracks, such as who sent it (full name plus email address), when it was sent, who received it, when it was opened, any distribution lists used, etc. All of these data are called metadata and are just as necessary to the record as is the text. When records are placed in a recordkeeping system, the attendant metadata also must be stored.

Attachment

Attachment refers to any file which accompanies an email message. Attachments can exist in a large variety of formats, the number of which continues to increase as software is superseded or new software developed. Files may be text, graphics, spreadsheets, video, audio files, Web pages, compressed files, or any combination of these mediums. Like emails and metadata, the attachments of emails must also be retrievable in an unaltered state.

Discovery

Discovery refers to the compulsory disclosure of records believed to be associated with litigation. Likewise, e-discovery refers discovery that focuses solely on electronic records, emails primary among them. The legal risks and increasing costs associated with discovery and e-discovery make the establishment of a statewide email management policy all the more crucial. The federal and State rules of procedures now compel civil litigants to preserve and produce electronic evidence on demand.[1]

RECORDS MANAGEMENT AND RECORDKEEPING SYSTEMS

Email records should be placed in some kind of recordkeeping system. A recordkeeping system can sort records according to purpose and retention schedule, provide security against unauthorized access or destruction, facilitate efficient retrieval, and preserve important information. Once the record is in the system, the original electronic source record that may still exist in the sent or received box or on backup tapes should be destroyed.

Email Systems

Email management systems rely on the user to organize and purge emails via a system of folders, tags, or labels or through similar options. Managing email within the email electronic system is technology that is readily available and requires minimal training. Folders, tags, and labels can align with record function and retention category. It requires the user take action to identify and set up email records. After the records meet their retention period, obsolete records are deleted according to their retention schedule and historical records are transferred to the State Archives' custody. User-managed accounts within the email system is a simple, electronic recordkeeping system; but it is labor intensive. Records management policy may be compromised through employee oversight or negligence or, in some cases, intentional breach of ethics.

[1] Federal Rules of Civil Procedure, Fed. R. Civ. P. 37 "(e) Failure to Provide Electronically Stored Information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."
Utah Rules of Civil Procedure, Utah R. Civ. P. 37 "(g) Failure to preserve evidence. Nothing in this rule limits the inherent power of the court to take any action authorized by Subdivision (b)(2) if a party destroys, conceals, alters, tampers with or fails to preserve a document, tangible item, electronic data or other evidence in violation of a duty. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

Centralized Systems

Software that is purchased, developed, or customized to automate the records management functions offers greater control over when and how records are viewed by an organization (not just the creator), destroyed, or transferred to the State Archives. This type of software centralizes many functions that are then overseen by a professional records manager. Central control of email records management alleviates issues such as duplicates and tends to better organize extended correspondence among multiple users while also ensuring legal compliance. The oversight of deletion or purging of emails from the system is also concentrated among trained records managers as opposed to relying on every employee in each agency to maintain compliance.

There are several centralized email management options available to large operations such as State governments that significantly reduce the risks associated with end-user systems. The first option is a Local Area Network (LAN). LAN storage relies on each user of an email system to manually move individual emails out of a mailbox and into the shared file directory structure. This option leaves the door open to some of the risks associated with end-user management, but it has the advantage of some central oversight, especially in regards to retention and disposition.

A second option is email archiving software, which is capable of organizing incoming and outgoing emails and sending them to centralized servers. The benefits of such software lay largely in automation and in reduction of the amount of emails that need to be stored on individual computers and online servers. The downside to such software is that its focus is solely on emails, which necessitates a separate system for other types of electronic records.

A third option is an Electronic Document Managing System for Enterprise Content Management (EDMS/ECM) to act as a central archive for all types of electronic records. Many of these types of systems are capable of both automatically managing email traffic and tracking retention and disposition of emails and other types of electronic records.

Agencies may choose whichever recordkeeping system fits best working in conjunction with the State Archives and the Department of Technology Services (DTS). Recommended functionality requirements that these systems has been prepared by the U.S. Department of Defense, titled the 5015.2 standard.[2]

POLICY COMPONENTS

The goal of an email records management system is to manage email from creation or receipt to destruction or permanent preservation. The policy that governs that program must address—but not necessarily be limited to—the following points:

[2] Joint Interoperability Test Command, Records Management Application, ***http://jitc.fhu.disa.mil/recmgt/standards.html***. The current version of DoD 5015.02-STD, signed 25 April 2007, defines the basic requirements based on operational, legislative and legal needs that must be met by records management application (RMA) products acquired by the Department of Defense (DoD) and its Components. It defines requirements for RMA's managing classified records and includes requirements to support the Freedom of Information Act (FOIA), Privacy Act, and interoperability. This standard is recommended by the National Archives and Records Administration as well as the Utah State Archives.

Essential Elements of the Email Management System

Each State agency should require, via policy, administrative rule, or statute, that it use an approved electronic records management system or develop a policy of their own that is in compliance with the baseline standards of said system. A management system includes the hardware, software, and storage medium used to manage email, and the policy describes how the system is used and the records it contains. To ensure that all essential emails are accessible within the management system, the policy must require that all State business is conducted on computers and devices that are connected to an authorized management system.

Evaluating and Appraising Email

Several issues must be considered when determining how emails fit within a records management system. The most important of these questions is whether an email is a record. If the email was sent or received as part of a State business transaction, be it an interagency transaction or business with an entity outside of State government, it is considered a record. According to the Government Records Access and Management Act (GRAMA), Utah Code § 63G-2-103(22)(a), a record is:

> a book, letter, document, paper, map, plan, photograph, film, card, tape, recording, electronic data, or other documentary material, regardless of physical form or characteristics, that is prepared, owned, received, or retained by a governmental entity or political subdivision where all of the information in the original is reproducible by photocopy or other mechanical or electronic means.

Principally, email that is work-function related, and has administrative, legal, fiscal, or historical value, is a record. Conversely, documents that are considered non-records include: drafts, personal notes or communications, proprietary software, copyrighted material, junk mail, commercial publications, and personal daily calendars. Personal messages, as defined by Utah Code § 63G-2-103(22)(b), created or received through email systems do not require a formal retention schedule. The recommendation is to destroy upon receiving or sending.

Once an email is determined to be a record, it must be decided whether it is the record copy of that correspondence. Duplicate copies can be discarded at any time, and retention schedules apply to the official record copy of that email. The same kind of consideration should be given to attachments within emails. It is important to note that attachments may well have their own retention periods, and thus a determination needs to be made regarding whether the attachment exists in other formats (paper, PDF, word-processor file, etc.) and which of the formats is the record copy. Like email, attachments that are duplicates can be discarded when the administrative need of the recipient has ended.

Primarily, within government, the outgoing (sender's) copy of an email is the record copy, and the copy with the longest retention. This retention holds until a response is made to the initial email, at which point a series of correspondence (thread) is created. In such instances, the last email in the thread—the one containing the entirety of the correspondence between two or more persons—becomes the record copy and thus the copy with the longest retention period. However, email can be broadcast to hundreds of people at once, and each of those duplicates should not be

saved. Only those recipients who then respond to the correspondence need save copies. Incoming (the recipient's) email originating from outside the government is the record copy.

If it is decided that the email is the record copy, then the record series to which it belongs needs to be determined. The record series will indicate the email's legal retention period and its ultimate disposition (i.e., destroy or permanent preservation and access).

Access and Retrieval

A current method for finding and retrieving email uses the search functionality of the email system. Emails can be searched for author or recipient name, time periods, subject as derived from the message title, and a full text search of the email, but not the attachments. To make searching more reliable and efficient, email and related attachments judged to be worth keeping should be ingested into an email records management system that provides faster and enhanced search capabilities.

In order to provide accessibility and promote efficient searching mechanisms, all outgoing emails related to State business must have a subject line that clearly reflects the content of the email. Index terms to the metadata may be applied to further promote ease of access.

Disposing of all non-record emails greatly reduces the amount of email that requires access and retrieval resources. Some systems provide capabilities for employees to make these categorical decisions rapidly and with high levels of automation. Currently most retention decisions are managed manually at the discretion of the employee and according to specific agency policies within the context of the current email environment.

Email saved on employee equipment should not be routinely purged by IT personnel and should not be automatically discarded upon termination, but preserved until such time that they can be reviewed and appropriate retentions applied to the records.[3] Approved retentions and appropriate disposition for destruction of these types of email should be established to minimize storage requirements for the State.

E-discovery

Both the federal and Utah Rules of Civil Procedure expressly provide for the discovery in litigation of all discoverable electronically created or stored information, including emails, in their electronic format. Electronically stored or created information can be regularly destroyed without penalty under these rules if the destruction was pursuant to a reasonable electronic records management system that is consistently implemented and followed within the agency.

[3] POP (Post Office Protocol) and IMAP (Internet Message Access Protocol) are standard methods for retrieving and potentially saving email messages on a computer or network. Most mail servers are set up to recognize the protocols and Gmail is no exception. Depending on settings available to each individual, POP may be used to download or copy mail messages to an email client such as Microsoft Outlook. One may also disable it entirely. IMAP is used for a more dynamic, two-way connection where one accesses email in a client that is continuously updated by the mail server. It may also be disabled by the individual. One or both of these protocols are used for mobile device access, likely depending on the operating system and default settings. IMAP is preferred by Google.

This "safe harbor" is suspended, however, when a "litigation hold" has been, or should have been, put in place. A litigation hold is an internal directive to preserve all relevant information, including electronically created or stored information, which is in the possession, custody, or control of the agency.

The obligation to implement a litigation hold is triggered as soon as the agency knows, or should have known, that litigation regarding the matter at issue was reasonably foreseeable. Once a litigation hold is implemented, all deletion or destruction protocols with regard to electronically created or stored information that may relate to the matter at issue must be immediately suspended. Those records must thereafter be preserved in their electronic format until any litigation is concluded or the litigation hold is appropriately lifted.

The failure to properly implement a litigation hold where litigation is reasonably foreseeable, or failing to comply with such a hold after it is implemented, can result in significant penalties or sanctions. Such penalties or sanctions can include: payment of the costs of recovering, sorting and producing the lost information from backup tapes; payment of all or part of the other side's attorney's fees; where the failure to preserve was known and intentional, significant monetary penalties against the agency and/or its officers, managers, and attorneys; an adverse inference jury instruction, advising the jury that it can presume that lost information would have been favorable to the other side; and, in extreme cases, entry of judgment for the other side.

To avoid such sanctions or penalties, the following procedures should be implemented:

> As soon as an employee of an agency becomes aware of pending litigation or of information that suggests the risk of future litigation (i.e. correspondence from former, particularly terminated, employees or correspondence from a patron regarding or resulting from an interaction they perceive as especially egregious), even if the employee believes that such possibility is remote, the employee should report that information to the appropriate manager or supervisor.
>
> In turn, as soon as a manager or supervisor obtains such information, whether from an employee or independently, that information should immediately be reported to the executive director of the agency, and to agency legal counsel.
>
> Agency legal counsel, in consultation with the executive director and such others within the agency as may be appropriate, shall make the determination as to whether litigation is, in fact, reasonably foreseeable. If it is, then a litigation hold shall be issued by agency legal counsel to the agency.

As can be seen from the foregoing, upon the issuance of a litigation hold, the electronic records management system must have the ability to identify, segregate, archive, and preserve discoverable electronically created or stored information, including emails, in their original electronic format, including all metadata. The electronic records management system must be able to do this without impeding or interfering with the normal operation of the system with regard to records not affected by the litigation hold.

Google Message Discovery (GMD)

Gmail provides an optional application that creates an irrefutable repository of all email of a user's account: Google Message Discovery (GMD). GMD automatically retains *all* sent and received email of an account in a repository separate from the user's Gmail account. It provides a means that email, and attachments, may be searched and put on hold in instances of pending litigation or even GRAMA requests. It eliminates the need for individual employees to make decisions about whether or what email records to retain. *Copies* of email can be taken from the repository for use, but the emails in the repository cannot be in any way altered, manipulated, or deleted.[4] Retention schedules cannot be applied to email in the GMD repository but, instead, retention is subject to the period defined by the GMD application.

Storage

To enable a capable email archiving and retention practice at the State, provisions should be established for each of the following types of storage required:

> **Category 1**: Centralized email storage for active email (e.g., the last 60 days) with automated retention and destruction rules consistently implemented to minimize excessive storage requirements.
>
> **Category 2**: Agency or multi-agency storage for active email at the post office level.
>
> **Category 3**: Centralized transitional storage for all email assigned to specific records groups by agency personnel.
>
> **Category 4**: Centralized Archive email repository storage for email that has been transferred to the State Archives and assigned to specific record groups and are accessed through a Records Management System.
>
> **Category 5**: Archival storage for archived email that has been stored on computers used by employees that have terminated their employment with the State for whatever reason.

Storage for Categories 1, 2, and 4 needs to be high speed, high availability, on demand storage environments. Storage for Categories 3 and 5 can be met by less expensive disk and/or tape storage environments.[5]

All of these storage environments should be backed up on established schedules using least-cost automated storage procedures. Stored email must also include relevant document attachments.

[4] GMD retains *all* emails of an account holder, including copies, personal email, and non-records. An agency should give careful consideration and balance the risks of retaining all emails of an account holder outside of the discovery process. In an efficient recordkeeping system, non-records should be disposed of immediately and not kept. An agency cannot select unique email within GMD for disposal, resulting in the probability that some records will be retained beyond the retention period.

[5] Upon request, DTS provides copies of backup tapes to State agencies. As backup tapes, these are only kept for up to two weeks and contain records of mixed record series with different retention periods.

Retention and Disposition

The practice of deleting email without regard to content is in contravention of legally established retention schedules. Retention schedules are created to account for any administrative, fiscal, legal, or historical value that may be contained in a record so that it may be disposed of appropriately. General retention schedules are designed to cover the needs of common records across all agencies. The following general retention schedules currently are used for various types of correspondence, including email:

> **Transitory Correspondence**: Incoming and outgoing correspondence, regardless of format or mode of transmission, related to matters of short term interest. Transmittal correspondence between individuals, departments or external parties containing no final contractual, financial or policy information. This correspondence does not impact agency functions. When resolved, there is no further use or purpose.
> Retention: Retain until administrative need ends and then destroy.[6]
>
> **Administrative Correspondence**: Incoming and outgoing business-related correspondence, regardless of format or mode of transmission, created in the course of administering agency functions and programs. Administrative correspondence documents work accomplished, transactions made, or actions taken. This correspondence documents the implementation of agency functions rather than the creation of functions or policies. Business-related correspondence that is related to a core function with an associated retention schedule should follow the associated schedule.
> Retention: Retain for 7 years and then destroy.[7]
>
> **Executive Correspondence**: Incoming and outgoing business-related correspondence, regardless of format or mode of transmission, that provides unique information relating to the functions, policies, procedures or programs of an agency. These records document executive decisions made regarding agency interests. Executive decision makers may include the Director, Chief Administrative Officer, Public Information Officer or other internal administrators as identified by the executive office.
> Retention: Permanent. May be transferred to the State Archives.[8]

Correspondence categories typically are easy to apply, however a more content-based approach to retention schedules—reflecting the widespread subjects and applications in electronic correspondence—for records groups also is needed. Other general retention schedule record series may be more appropriate to specific record groups, such as case files, and agencies may work with the State Archives in establishing unique retention schedules to fit specific needs of their operations.

[6] Utah State General Records Retention Schedule, Transitory correspondence (item 4-11).

[7] Utah State General Records Retention Schedule, Administrative correspondence (item 4-12).

[8] Utah State General Records Retention Schedule, Executive correspondence (item 4-10).

Preservation

Utah law requires that records are accessible for the full extent of their approved retention periods. Preservation of electronic records, including email, even for short-terms can be an issue because of technological changes and media degradation. Open-source solutions are ideal for meeting this requirement. Adopting open source products facilitates migration or conversion of email systems.

One strategy is the use of XML. Essentially, scripts are run against the transmittal copy of the email, with the message, attachments, and metadata captured and wrapped with XML. The XML files then are placed in an electronic recordkeeping system. Another strategy is to save the email in MBOX or EML files, which are text files that can be opened in any text editor. Most email clients understand MBOX and EML formats and support them natively, so email can be viewed in a familiar environment, with attachments separated from the main body of the email for easy access. Recordkeeping systems which accept MBOX, EML, or XML forms of the data should be able to parse fields for reuse in the recordkeeping workflow, including searchability.

The State Archives recommends that email with long retention periods be transferred from the email system into a recordkeeping system for retention and preservation. The State Archives has tools available that can retain and preserve email. Historical email records should be transferred to the State Archives at the end of their administrative use.

Chats

Many email systems support a chat function. Unlike email, chats are live-time conversations which enables users to communicate in real time. Email systems provide settings to save chats for future reference, recording conversations in the system.

Recorded chats are subject to the same requirements as email, including determining the content as a record or non-record, retention, and disposition. A user should keep in mind that even if he or she does not save a chat, it could be saved by the other party(ies) in the conversation.

Appropriate Use

Email within State government is subject to the existing Department of Technology's *Acceptable Use Rule*[9], which establishes guidelines for appropriate use of computing resources and content on State systems. State policy allows some limited personal use of email systems so long as such use is consistent with the *Acceptable Use Rule*. State provided email is considered to be the primary venue for conducting State business, and such business should not be conducted using third party email providers. As a matter of principle, State email users are expected to conform to the following:

- State business conducted via email should use established and approved State email systems.
- Private business activities should never be conducted using State email systems.

[9] [5] Title R895. Technology Services, Administration. Rule R895-7. Acceptable Use of Information Technology Resources.

- Email should respect gender, creed, race, ethnic background, or other identifying characteristics.
- Email should be preserved and managed consistent with State records policies and rules.
- Email should respect the integrity of computing systems.
- Individual user accounts and passwords must be safeguarded.
- Agency and State email policies should be integrated into existing Web mail and network access policies to strengthen and give visibility to email policies.

THE BACKLOG

Many State agencies have an extensive backlog of emails. Due to risks associated with e-discovery and litigation, it is equally important that these records be managed retroactively according to established records retention periods. The scale of backlogged emails, and the risks associated with these records, will vary from agency to agency, as will the complexity of bringing them up to newly-established standards.

Once standards for records management are established, those records most at-risk should be prioritized and addressed accordingly.

Often backups can be downloaded or emails simply relocated to the new, centralized system. In cases of obsolescence or backup failure, data recovery specialists can be contracted to restore information in current formats or media.

SUMMARY

Email must be managed not as a physical format with one-size-fits-all requirements, but as content that has specific value or non-value to an agency. To manage email, State agencies should work to customize a centrally-managed, open-source, records management system to support their individual needs and obligations. Such a system must address the issues of records evaluation; appraisal and retention; appropriate use; preservation and issues of obsolescence; access and retrieval; and e-discovery.