

SECTION 34 ELECTRONIC RECORDS RETENTION

A. PURPOSE:

The Government Records Access and Management Act (GRAMA, UCA § 63-2-102) states that the public “has a right of access to information concerning the conduct of the public’s business.” GRAMA also maintains “the right of privacy in relation to personal data gathered by governmental entities” and establishes the rules for retaining and disclosing the information.

Common law and various court rules require parties to a lawsuit to preserve, maintain, and produce “evidence” related to a lawsuit. The Federal Rules of Civil Procedure and recent federal court cases require parties (and in some cases non-parties) in a federal lawsuit to also preserve, maintain, and disclose all “electronically stored information” (ESI) that is relevant to a claim or defense in a lawsuit once a party has received notice of the suit or has received sufficient information to realize that a lawsuit is to be filed.

The purpose of this policy is to acknowledge the requirements of the law and to ensure that County officials and employees understand the requirements and understand that the County, as an entity, as well as its officials and employees in their official capacities, must comply with the preservation, maintenance, disclosure, and disposition requirements pertaining to County records, including ESI.

B. POLICY:

1. This policy establishes guidelines and standards setting forth the requirements and responsibilities for the maintenance, storage, litigation holds, and destruction of County records centrally stored in digital, optical, magnetic, or other forms of electronic media.
2. All County departments and personnel shall adhere to this policy and the incorporated County Records Retention Schedule when storing or requesting the destruction of County records.
3. ESI shall be disposed of after it has fulfilled its purpose and met the required retention period.
4. ESI may not be destroyed if any litigation, claim, negotiation, audit, open records request, administrative review, or other action involving the record is initiated before the expiration of a retention period, until the completion of the action and the resolution of all issues that arise from it, or until the expiration of the retention period, whichever is later.

C. DEFINITIONS:

1. “ESI” means Electronically Stored Information.

2. “County Electronic Record” means a record created, generated, sent, communicated, received, or stored by electronic means on County servers.
 - a. “Record” means recorded information, regardless of medium or characteristics, made or received by an organization that is evidence of its operations, and has value requiring its retention for a specific period of time. Recorded information, in any format, that is created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business is considered a record.
 - b. Characteristics of electronic records include: authenticity (it is what it says it is), reliability (it can be trusted as a full and accurate representation of the transactions or facts), integrity (it is complete and unaltered), and usability (it can be located, retrieved, presented, and interpreted).
 - c. Common formats for electronic records are: text-based documents, databases, spreadsheets, web pages, drawings and diagrams, maps, electronic mail (email), etc.
 - d. “County Electronic Record” does not include:
 - (1) a personal note or personal communication prepared or received by an employee or officer of a governmental entity in the employee’s or officer’s private capacity;
 - (2) a temporary draft or similar material prepared for the originator’s personal use or prepared by the originator for the personal use of an individual for whom the originator is working;
 - (3) material that is legally owned by an individual in the individual’s private capacity;
 - (4) material to which access is limited by the laws of copyright or patent unless the copyright or patent is owned by a governmental entity or political subdivision;
 - (5) proprietary software;
 - (6) junk mail or a commercial publication received by a governmental entity or an official or employee of a governmental entity;
 - (7) material that is cataloged, indexed, or inventoried and contained in the collections of a library open to the public, that is maintained in electronic format;

- (8) a daily calendar or other personal note prepared by the originator for the originator's personal use or for the personal use of an individual for whom the originator is working;
- (9) a computer program that is developed or purchased by or for any governmental entity for its own use;
- (10) a note or internal memorandum prepared as part of the deliberative process by a member of the judiciary, an administrative law judge, or a member of any other body charged by law with performing a quasi-judicial function;
- (11) a telephone number or similar code used to access a mobile communication device that is used by an employee or officer of a governmental entity, provided that the employee or officer of the governmental entity has designated at least one business telephone number that is a public record as provided in Section 63G-2-301 of the Utah Code;
- (12) an extra copy of recorded information maintained only for reference; and
- (13) personal, temporary, or transitory emails.

D. PROCEDURES:

1. Records Retention Schedule - County Records shall be retained pursuant to the current County General Records Retention Schedule prepared by Utah State Archives, as well as all applicable Federal record-keeping requirements. In addition to this requirement, the Information Technology Department shall permanently retain all County electronic records of County elected officials and shall retain for ten (10) years all County electronic records of County employees, unless otherwise directed by the County legislative body.
2. Electronically Stored Information - ESI.
 - a. Provision for adequate maintenance, disposal, and preservation of electronic records should be built into work process and tools, so that electronic records management is a routine and time-efficient activity.
 - b. Electronic records should be created and maintained in reliable and secure systems. The County departments shall identify systems or applications that create and maintain records. The development, modification, operation, and use of these systems/applications should be documented and coordinated with the Information Technology Department to ensure reliability and security of records over time.
 - c. All County departments shall take appropriate measures to prevent unauthorized access to electronic records.

- d. Appropriate metadata about electronic records must be captured at the time of creation. Electronic data must be captured in such a manner as to document the context, content, and structure of electronic records.
 - (1) Context establishes who created the record and the transaction of which it was a part.
 - (2) Content is the actual data.
 - (3) Structure is the format of the record. Structure must be captured so that the record can be migrated into the latest generation of hardware and software as necessary.
- e. In most cases, electronic records should be maintained in electronic form.
- f. As technologies change, the County Information Technology Department is responsible for migrating ESI forward.
 - (1) Records should be routinely monitored in order to identify any formats that are at risk of obsolescence.
 - (2) Migration of records should be planned, quality controlled, and documented.
 - (3) Where records are in unique or legacy formats/systems with no migration paths available, they must be supported by the County during their retention period, unless converted to a non-electronic format.
- g. Digital records must be secure and tracked throughout the preservation process. The preserver should implement security measures to ensure that the records being preserved are not compromised during any preservation process.
- h. Digital records preservation programs should be flexible. The preserver should seek to base digital records preservation approaches on non-proprietary technologies to avoid loss of control over County-owned information as a result of changed commercial arrangements in the future.
- i. The original hard copy of a permanent record (source document), that is converted into electronic format, can be destroyed after a minimum of 5 days has passed since the conversion, and the department is confident that the conversion has been completely successful.
- j. Electronic records shall be saved and stored on designated server-based personal and departmental workspaces (“H” drives, “X” drives, etc.) or in designated network databases. These server workspaces fulfill the requirements of records retention, audit, and discovery since they are backed up, indexed, and can be centrally searched.

- (1) Official electronic records shall not be permanently saved on any other media, including workstation hard drives, USB-attached memory devices, media drives, etc.
- (2) Workstation hard drives are to be used only for the workstation operating system, County-licensed application program files, and associated temporary files appropriate to allow the workstation application programs to function correctly. In no event should official electronic records or non-County-licensed programs be saved or installed on workstation hard drives.

3. Electronic Mail (E-mail).

a. Definition - E-mail is a means of sending messages between computer devices using an established network through the County's email server.

- (1) This information consists primarily of messages, but may also include attachments such as calendars, directories, distribution lists, word processing documents, spreadsheets, and other electronic documents.
- (2) E-mail is stored in a digital format rather than on paper and is retrievable at a future date.
- (3) Due to format, e-mail permits communication and transmittal of up-to-date information similar to the telephone. Unlike current telephone features, e-mail creates a record of the information that is being transmitted.

b. Retention Guidelines.

- (1) E-mail messages sent and received by County employees fall within four broad categories:
 - (a) 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.
 - (b) 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.

- (c) Records with a Permanent or Permanent/Archival retention period.
 - (d) 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.
- (2) Retention guidelines for each of these categories are as follows:
- (a) Transitory messages - A transitory e-mail message shall be deleted as soon as it has served its purpose.
 - (b) Less than Permanent Records - Follow the retention period for equivalent hard copy records as specified in the County's approved retention schedule.
 - (c) Permanent or Permanent/Archival Records - The record must be converted to a readable permanent format. If an email is determined to be an official record, it will be:
 - (i) The outgoing (sender's) copy of the email.
 - (ii) The email containing the entirety of all the correspondence between all parties when an email thread has been created.
 - (iii) The incoming (recipient's) email when originating from outside Tooele County government's system.
 - (d) Executive Correspondence - Permanent and may be transferred to the State Archives.
 - (e) Elected officials and administrative officers are responsible for instructing their employees in determining which e-mail messages fall into each of the three categories, in using retention schedules, and in the process for destruction. Retention is the responsibility of the sender/recipient of the email, not the backup process.

(3) Legal Considerations - Disclosure of Email.

- (a) Public officials, administrative officers, and employees should keep in mind that e-mail messages sent as part of their job assignment are not private and may be discoverable communications.
- (b) Since messages may be retained at different locations, users should remember that their communication can be retrieved during formal discovery processes.
- (c) Discretion, therefore, is an important consideration when using this or any other technology to send, record, and/or retain communications.

(4) E-mail - Neither Secure Nor Confidential.

- (a) Electronically transmitted information travels through many networks and many different computer connections.
- (b) This information is not secure and should not be considered private.
- (c) County departments are advised that there may be risk involved in using e-mail to deal with confidential issues.
- (d) Agencies must be aware of all applicable statutory or regulatory requirements that would prohibit the disclosure of certain information. Of special concern is the confidentiality of individually identifiable health and personnel information. Agencies must be aware of this when transmitting this information by email.

4. Voice Mail.

- a. Voice mail can be considered a type of electronic mail communication. In this case, the message is recorded in an audible rather than a visible format.
- b. Voice mail is primarily transitory in nature. Voice mail messages are automatically deleted from the server after ten days, unless deleted earlier by the employee or a longer retention period has been specifically requested by the user. All voice mail messages may be deleted as soon as the message is no longer needed. Employees wishing to retain information contained in voice mails may save the voice mail in a specified folder on the voice mail server or may copy the desired information onto a network drive.
- c. A voice mail retained in a specified folder on the voice mail system or a network drive may be deleted at any time, unless subject to a hold directive issued pursuant to this policy. All messages subject to a hold directive shall not be deleted, altered, or destroyed until written authorization has been received.

5. Electronic Personnel, Discovery, and Litigation Holds - Electronic discovery refers to the discovery of electronic documents and data. Electronic documents include email, web pages, word processing files, computer databases, and virtually anything that is stored on a computer. The same rules that govern paper discovery, govern electronic discovery.
 - a. The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation.
 - b. Upon determining that litigation or an investigation is threatened or pending and has triggered a preservation obligation, the County Attorney's Office shall take reasonable steps to communicate to affected persons the need for and scope of preserving relevant records (both electronic and hard copy).
 - (1) An appropriate notice shall be effectively communicated to an appropriate list of affected persons.
 - (a) The notice shall be sent to those departments and employees reasonably likely to maintain documents relevant to the litigation or investigation.
 - (b) Notice shall also be sent to a person or persons responsible for maintaining and operating computer systems or files that have no particular custodian or owner but may fall within the scope of the preservation obligation.
 - (2) The notice need not be a detailed catalog of information types to be retained. Instead, it should sufficiently describe the kinds of information that must be preserved so the affected custodians of data can segregate and preserve identified files and data.
 - (3) The notice shall not trigger preservation of all documents, only those affected by the preservation obligation.
 - c. All County employees notified of the responsibility to preserve documentation, electronic or otherwise, shall comply with all requirements contained in the notification.
 - (1) When preservation obligations apply to documents and data spanning a significant or continuing time period, organizations should analyze whether special steps are needed to deal with hardware that might be retired if it contains unique relevant documents.
 - (2) The preservation obligation, except in extreme documented circumstances, shall not require the complete suspension of normal document management policies, including the routine destruction and deletion of records.

- d. All documents and information subject to a hold directive shall not be deleted, altered, or destroyed until written authorization has been received by the holder of the records in question. Any existent hold shall be reviewed on an annual basis by the County Attorney's Office and the Information Technology Department.

6. Responsibilities.

- a. Each County department and all County employees and elected officials are responsible for compliance with County policies, including this policy relating to electronic records retention, maintenance, and destruction.
- b. Compliance by the Information Technology Department specifically includes:
 - (1) Developing a security program for electronic records that is in compliance with industry standards.
 - (2) Developing capability for preserving any electronic County record resident in the system for its full retention period; or, there must not be any system impediments that prevent migrating the record to another electronic records system, in as complete a form as possible.
 - (3) Coordinating the documentation and destruction of electronic County records and disposing in a manner that ensures protection of any confidential information.
 - (4) Maintaining proper climatic temperature control for any storage of electronic media.
- c. Compliance requires a joint effort by all departments, records management and Human Resources personnel, and the Information Technology Department. Compliance includes:
 - (1) Providing mandatory training and materials during a regularly-scheduled training cycle for users of electronic records systems in the operation, care, and handling of the information, equipment, software, and media used in the systems.
 - (2) Developing and maintaining written documentation about institutional electronic records that is adequate for retaining, reading, or processing the records and ensuring their timely, authorized disposition.
 - (3) Annual review and destruction of electronic records that have met the required minimum retention period or continued retention until destruction is operationally practical.
 - (4) Media used to store electronic County records will be wiped before the hardware passes out of the County's custody.

7. Destruction of ESI.

- a. When information that is stored electronically has fulfilled the retention period, the information can be erased.
- b. The procedure and schedule for erasure is provided on the retention schedule. By erasing the information, or recording over it, the media is free for reuse.
- c. Erasure of electronic media is considered destruction.