



RECORDS MANAGEMENT SERVICES

ELECTRONIC MESSAGING GUIDELINES (E-MAIL)

Electronic Messaging is a set of communication processes used to relay information among the users of computers. Electronic Mail (E-Mail) is one form of Electronic Messaging. Electronic Messaging messages, delivery information, and addresses. The computer programs that implement Electronic Messaging on desk top computers often include other functions such as calendar, notes, task assignments, appointments, telephone messages, possibly forms routing, and publication distribution. Most, if not all of the packaged functions are intended to facilitate the communication of information among people. The combination of messages and services is referred to as an Electronic Messaging System. Such systems allow for the creation, routing and delivery of pieces of electronic information. Electronic Messaging can take place among a few people located within an office or it can be expanded to occur internationally.

Since Electronic Messaging is relatively new as a practical reality to the employees of the State of Colorado, there are a number of issues that can effect how and when to use Electronic Messaging. This document will attempt to address some of the most common questions.

Are Electronic Messages Public Record?

Electronic Messages take many forms. Including "yellow stickys", memos, and transmittal letters. Electronic Messages may or may not be public records depending upon the content. Both the author and the recipient must use their judgement as to the nature of the material and take appropriate steps to treat the Electronic Messages just as they would any other form of information. Under Colorado's public records law, many Electronic Messages may be public records. The definition of public records in CRS 24-80-101 includes "all books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, made or received by any governmental agency in pursuance of law or in connection with the transaction of public business....". If there are questions as to an individual Electronic Message's status in relation to the public records law, consult your organization's document retention policies, the State Archivist and/or your organization's legal counsel.

What about retention and disposition of Electronic Messages?

The retention of records stored in electronic records systems, including Electronic Messages, is governed by CRS 24-80-101 to 24-80-115 (Public Records Law). Electronic Messages are to be retained and deleted in accordance with these statutory procedures. As a practical matter, Electronic Messages should be removed from the Electronic Messaging system to be located with other documents having similar retention characteristics. The costs associated with retaining all prohibitive and unwarranted. If the Electronic Messages were retained for long periods of time within the system then it might be necessary to maintain old versions of software as the Electronic Messaging systems are upgraded and replaced.

Electronic Messaging should not be retained within the Electronic Messaging system for extended time periods. The message text should be reviewed then moved or deleted on a regular basis; normally less than ninety days.

Do you have suggestions concerning storage and preservation?

Electronic Messages are typically stored on-line. Since some messages may be stored in an encrypted format, future access must be considered. When Electronic Messages are reviewed for retention, the relocation must be to an area that has a sufficient life span to insure the retention of the electronic Messages for as long as they are of value to the agency using them. Further, when they are relocated they should be stored in a manner that no longer requires proprietary software to retrieve the document, (i.e. remove encryption and store in a standard text format or print the document to disk if the contents cannot be converted to a standard text format).



RECORDS MANAGEMENT SERVICES

Records officers, program managers, and systems managers have the responsibility for establishing standards for indexing information which facilitates access to stored Electronic Messages just as they have the responsibility for other forms of stored documents.

What about appropriate use, privacy, and confidentiality?

Users of Electronic Messaging systems are responsible for the appropriate use of the systems. The following suggestions should assist users in determining appropriate use of the Electronic Messaging systems:

- The Electronic Messaging systems are intended for business purposes only. You should only use the Electronic Messaging systems to conduct official State of Colorado business.
- If you are preparing an Electronic Message which you do not want to be forwarded, clearly mark the message "Do Not Forward - For Your Eyes Only". If you wish to forward a message, it is always good etiquette to ask for the author's permission.
- Do not use Electronic Messages for private or confidential matters. There is no guarantee of privacy or confidentiality. There are other avenues of communication available for matters requiring privacy and/or confidentiality.
- Although we are used to a mail system which is quite private, the privacy afforded employees using Electronic Messaging systems is minimal. Since the Electronic Messages could easily be public records, the only privacy a state employee can expect is that privacy afforded through disclosure exemption of the CRS.
- Recent court rulings have given employers broad rights to view the contents of employee Electronic Messaging mailboxes. The reason for viewing include but are not limited to the following; to monitor Electronic Messages for enforcement reasons or to access in an employee's absence.
- A good rule of thumb should be to never use an Electronic Messaging system to send a message that would be the source of embarrassment to either the sender, recipient or agency if the message were to be seen by others.
- Each department should develop and distribute a policy concerning Electronic Messaging. This can avoid misunderstandings and conflicts concerning Electronic Messaging issues.
- Password security at the terminal is very important. Leaving a terminal "signed on" or leaving the password available in an obvious place, gives any "passer-by" the opportunity to send an Electronic Message which appears to be authored by whoever left the terminal (password) unsecured.