COLORADO ATTORNEY GENERAL'S OFFICE
Information Systems

TITLE: Email Retention and User Guidelines

ORIGINATOR:	REVIEWER:	APPROVER:
Tony Jones, **Chief Information Officer**	**Cynthia H. Coffman** **Chief Deputy Attorney General**	**John W. Suthers** **Attorney General**
ORIGINAL EFFECTIVE DATE: **March 21, 2001**	**DATE LAST REVIEWED:** **July 2, 2012**	**EFFECTIVE DATE THIS** **May 1, 2014**

OVERVIEW

Developed to maximize legitimate use of the electronic mail (email) system, and because the Office of the Attorney General is a government entity, this policy considers several factors in the use of email. They include: public disclosure, privacy, public records retention, ethics, business needs, and common sense. The policy statements that follow fall into five categories: privacy, acceptable use, security, retention, and monitoring/access.

PRIVACY

All email sent or received through the Department of Law's internal Microsoft Exchange email system is property of the Office of the Attorney General. Employees should have no expectation of privacy in using this form of communication, except for attorney-client privileged material. The federal Electronic Communications Privacy Act of 1986 prohibits interception of messages from groups outside the office, but the Act does not apply to intraoffice and "stored" electronic messages. Legal precedent has been established which supports an employer's right to access email because the employer owns the email systems.

Email messages may be considered "public record" under C.R.S. 24-72-203 and thus subject to public disclosure. They may also be subject to preservation requirements under C.R.S. 24-80-101 *et seq*.

ACCEPTABLE USE

Agency email systems are not to be used for transmission of information that promotes:

- Discrimination on the basis of race, creed, color, sex, age, national origin, religion, disability, or sexual orientation;
- Sexual harassment or sexual misconduct;

- Transmitting obscene materials;
- Copyright infringement;
- Personal political beliefs or political campaign activities;
- Any unlawful activity; or
- Dissemination of "chain letters."

Primarily use Department email systems to conduct Department business. Employees may use email systems to conduct other law related business such as providing periodic pro bono legal services in accordance with the Department of Law policy on providing such services, work on bar association work, or other public service work.

Employees may send incidental personal messages which are insignificant in cost and resource usage, provided they comply with statements in this policy. Examples of incidental personal use include (but are not limited to):

- Communication for those who are hearing-impaired (rather than using telephones);
- Notice of social and public service events, such as "Adopt-A-Family" fund-raisers, "Combined Fund" drives, blood drives, shared leave requests, etc.;
- Gatherings (lunches, birthdays, receptions, etc.); and
- Department-wide notifications used for communicating goodwill among employees (holiday greetings, congratulatory messages, etc.).

Email communications must be professional in content. The message sent may be printed and sent, or forwarded to others outside the office. The content and tone of a message reflects on the Attorney General's Office and the Attorney General.

Various types of email groups are set up to make communication within the office easier. These groups can be found in the address book of the email system.

Department employees have access to various types of confidential information, including attorney-client privileged communications, medical records, tax information, trade secrets, and grand jury information. Each section shall establish a policy that identifies the specific types of confidential information its employees routinely handle and establish procedures for transmitting this information via email, including any bars on such transmission and the types of confidential information that must be sent in an encrypted format.

All email sent between the Department's internal Microsoft Outlook email system and Colorado state agencies using the Google Apps for Government email system, including text within the body of the email or attachments, is encrypted by default and users do not need to take extra steps to secure such communications.

In accordance with this policy and any applicable section policy, email containing

confidential or sensitive information must be encrypted when sent to any recipient besides State of Colorado agencies using the state sponsored Google Email. This includes Colorado agencies that do not use Google email, other state or federal government agencies, private law firms or businesses, and private citizens. Department employees must use the Google/Zix encryption portal when sending emails that are required to be encrypted. No other system, such as Dropbox or Adobe SendNow, may be used to transmit such confidential information. To use the Google/Zix portal, type the word "encrypt" (no quotes necessary) in the subject line of the email. This will send the email to a secure portal from which the recipient can view the email and any attachments. From this portal the recipient can reply to the email and can forward it on to other Colorado state agencies, but cannot forward it to external parties.

Employees are expected to take precautions to prevent unauthorized use of their electronic mailboxes. Precautions include:

- Locking your workstation while away from your desk; and
- Logging out of the computer system/network before leaving the office.

Employees may not read or disclose the email of another employee where there is no substantial business justification.

Employees may not send email under another employee's name ("spoofing") without that employee's authorization.

EMAIL RETENTION AND DESTRUCTION

The Information Systems Unit (ISU) is responsible for backing up email data stores and providing disaster recovery capabilities. Employees are responsible for managing their Outlook email in accordance with this policy and any applicable Department and section policy regarding records retention and destruction.

Email retention in the Department of Law is based upon a mixed date and volume based approach.

- 1 gigabyte (gig) of space is allocated to each end user to manage their email volume. Items under the user's mailbox, including but not limited to the inbox, sent items folder, drafts folder, and deleted items folder, are included in this volume quota.
- All items older than 90 days in the inbox or any subfolders of the inbox including sent items, subfolders, drafts, etc. will be automatically deleted on a daily basis. Once deleted, these items are not recoverable.
- Items that are deleted manually are sent to the deleted items folder under the inbox. All items older than 1 day in the deleted items folder are automatically deleted on a daily basis. Once deleted, these items are not recoverable.

Enforcement

Enforcement of the email retention policy is based upon the space available to the end user within their 1 gigabyte quota.

- Below 95%, email operations operate as normal.
- At 95%, the end user receives an email alerting them that they are approaching their email limits and should purge their mailbox of unnecessary items.
- At 100%, the ability to send and receive email shuts off. No email is delivered during this period; senders to this email address receive a "bounce-back" email stating the email cannot be delivered.
- Send and/or receive services are restored as soon as the user manages their mailbox to below the 1 gig limit.

Long-Term Email Retention

End users will strive to maintain an organized email management system by following best practices and keeping emails only for as long as needed. It is vital that the end user chooses carefully what documents are saved, where to save documents, and how long they are saved to help with governance of server space.

- Emails of a non-essential nature should not be kept for more than 30 days.
- End users may archive emails using "Save As" through Outlook or the Adobe PDF Archiving functionality. Archived emails should be stored in the ProLaw Case Management System or in the appropriate directory on the P drive.

Email Organization

- Mailbox size is defined by the total volume of all items contained underneath the "Mailbox" heading in Outlook.
- Folders may be created within a user's mailbox to manage and organize emails but these folders are included in the retention policy mentioned above.
- PST folders are not allowed.

Recommended Practices for Classifying Email for Retention or Deletion

The easiest way to manage email is to determine how long each email will be useful so you can store it accordingly. Some received or sent email may be deleted immediately or a very short time after it's read, while other email may need to be kept for an extended period of time. It is likely, however, that many of the email messages sent and received in the course of the workday will be somewhere between these two extremes. It is suggested that email be considered in the following three broad categories:

1. **Transient Email**. Email that is personal in nature, of fleeting or no value, or otherwise not created or received in the course of state business is encouraged to be deleted immediately after reading, but in no event more than 30 days after receipt. This may include emails about lunch plans,

arranging a ride home, spam, advertising, or other non-work-related publications or notices.

2. **Administrative Email**. This is email that serves some state-related purpose, but also is transitory or of time-limited value because it serves a time-defined administrative purpose. This may include email about an upcoming meeting or a reminder of an approaching deadline. Retain this email until it is no longer of administrative value (the meeting has occurred, for example) and then delete it. Generally, it will not be necessary to retain email in this category for longer than 30 days.

3. **Intermediate Retention**. This is email that has more significant administrative, legal, or fiscal value. This email may include resource information for a case, information pertaining to a specific subject area or topic, information pertaining to a procedural aspect of the legal process, or any other information to which you may want to refer in the future. If it is necessary to retain an email in this category for longer than 30 days, it is good practice to remove it from your email inbox using any of the methods discussed in the "Long-Term Email Retention" section above.

Consistent with Department policy, any email that is the subject of a public records request shall be preserved from the date of the request regardless of any maintenance, retention, or deletion policy or practices utilized by the custodian for that email.

Junk Mail

Junk mail is managed primarily by the Postini Email Spam filter that is hosted by OIT and integrated with DOL's Outlook email system. Postini captures the majority of spam but DOL users may also use the Junk Mail Filtering functionality that is built into Microsoft Outlook.

The Postini Spam solution provides a daily Quarantine Summary that is delivered to end users' email inbox from "State of Colorado OIT." Users should review this daily summary and use the Postini web-based interface to flag as legitimate emails ones that have been identified as spam.

MONITORING/ACCESS

Other than normal audit trail activities, email monitoring or access does not take place except when conducted as part of:

- An authorized training program or planned application design;
- An official investigation into suspected misuse or unlawful activities;
- Network troubleshooting procedures (and where affected employees are knowledgeable of the activity);

- Research for CORA requests, or
- Follow up to an employee's departure from the agency, for a period of not more than two weeks.

When a supervisor believes there is a need to access an employee's email messages, that supervisor must submit a written request to the manager of ISU. In personnel or disciplinary cases, the Section Deputy, the Chief Deputy Attorney General, and the Human Resources Director also shall be notified. In such cases, the Chief Deputy Attorney General will notify the employee within 48 hours after access to his/her email messages, unless there is a need for security because of an ongoing investigation. If responding to a request from a law enforcement agency, a prosecutor should be consulted to determine the need for a search warrant.

When an employee leaves the agency or goes on extended leave and there is email that needs to be retained or an address book that should be passed on, the employee should contact ISU for assistance in exporting the email messages and/or address book to a file which can be accessed by another employee in his/her unit/section. If there is a legal hold on a departing employee's email, the employee or their supervisor shall contact ISU for assistance in preserving that email in a native format.