


| | | | |
|---|--|---------------------|--------------------|
|  | State of Connecticut Office of Policy and Management | | |
| Policy Title: | Electronic Mail Records Management Policy | | |
| Policy ID: | IT-REC-15-01 | | |
| Version: | 1.00 | | |
| Date Effective: | 6/15/2015 | Next Review: | 6/15/2017 |
| Scope: | Executive Branch Agencies | Authority: | Sec. 4d-8a, C.G.S. |
| Summary: | The purpose of this policy is to establish the standards for the management of email and attachments, consistent with existing records retention requirements. | | |

Scope

This policy covers all State of Connecticut Executive Branch and Higher Education agencies and employees whether permanent or non-permanent, full, or part-time (hereafter collectively referred to as "users") who access or use the state systems in the performance of their assigned duties.

This policy does not apply to the Judicial or Legislative Branches of government. However, these branches may consider adopting any or all parts of this policy for use within their own branches.

This policy does not change any existing records retention requirements as established by the Office of the Public Records Administrator within the Connecticut State Library. Therefore, this policy only applies to those electronic records that are deleted.

Authority

In accordance with section 4d-8a, C.G.S., the Office of Policy and Management (OPM) is responsible for developing and implementing an integrated set of policies governing the use of information and telecommunications systems for state executive branch agencies.

Background

Pursuant to section 11-8, C.G.S., the Connecticut State Library is responsible for establishing records retention and disposition policies and schedules. The Public Records Policy # 5: Disposition of Public Records issued by the State Library on November 28, 2011 is the authoritative source of guidance for the disposition of public records, including email messages. The following key terms are incorporated by reference in this policy:

"Public record" means any recorded data or information relating to the conduct of the public's business prepared, owned, used, received or retained by a public agency, or to which a public agency is entitled to receive a copy by law or contract under

section 1-218, whether such data or information be handwritten, typed, tape-recorded, printed, Photostatted, photographed or recorded by any other method. [Source: Sec. 1-200 (5), C.G.S.]

"Official record copy" means the original or official copy of a record that is retained for legal, operational, or historical purposes. For example, if records are kept in both electronic and hard copy format, the agency must identify the official record copy. [Source: ARMA International. Glossary of Records and Information Management Terms, 3rd ed. Lenexa, KS: ARMA International, 2007.]

"Non-record" means any item that is not usually included within the scope of official records. Examples of non-records are extra (duplicate) copies kept only for convenience, reference materials, and blank forms. [Source: ARMA, Glossary.]

This policy does not supersede any of the Office of the Public Records Administrator's approved records retention and disposition schedules. See Office of the Public Records Administrator General Letter 2009-02, Management and Retention of Email and other Electronic Messages, for more detailed information.

The unauthorized destruction, removal, alteration, or use of public records is prohibited, pursuant to sections 53-153 and 1-240, C.G.S. The agency in possession or control of the official record copy of each public record must request permission to destroy such public record once it has met its minimum retention period.

From time to time, it may be necessary for the state to request that the contents of certain email accounts be preserved, so as to safeguard such content from deletion or alteration. Any email account for which an in-place hold or preservation request has been authorized by an appropriate agency official and formally submitted to the custodian of a state electronic mail system, shall be exempt from deletion from the system until such time as the in-place-hold or preservation request is rescinded. The State Library may provide additional guidance to agencies on state employees, such as appointed officials, whose records may require permanent historical preservation.

Deleted Emails

Users are responsible for organizing their mailboxes and ensuring that any artifacts of an electronic mail system, such as individual emails, calendar invitations, tasks and so forth that meet the definition of public record are appropriately managed in accordance with the records retention rules. For the purpose of this policy, the term "deleted" refers to any artifact of an electronic mail system whereupon the user has determined that the artifact was no longer needed and has taken an action that makes that artifact eligible to be permanently expunged from the system.

Any artifact of an electronic mail system that has been deleted from a user's account shall be eligible to be recovered by that user for a period not to exceed 150 days from the date it was deleted. As necessary, Agency Email Coordinators are available to assist a user in the restoration of deleted email.

Electronic Mail System Back-up Data

In accordance with the State Library's General Letter 2009-2, back-up systems or tapes are not acceptable for the long-term retention of electronic messages. The purpose of backing up the state's electronic mail system is to ensure against the loss of valuable data in the event of a disaster or system failure and provide for the timely recovery of the system.

Each electronic mail system back-ups created on or after the effective date of this policy will be retained for approximately thirty (30) days, after which time, the contents of said back-up will no longer be retrievable or recoverable in any manner.

Compliance

Agency Heads are responsible for ensuring compliance with this policy and may appoint a responsible designee from within their agency for policy oversight and administration.

Services provided under this policy may be revoked when an employee has terminated his/her state service or due to a policy violation or if it is determined that access is no longer needed or beneficial to the agency.

Compliance with this policy is subject to audit by the Auditor of Public Accounts.

Additional Resources

This policy should be read together with the following to ensure a full understanding of State policy:

- *State of Connecticut Policies on Security for Mobile Computing and Storage Devices, Network Security Policy and Procedures;*
- *Acceptable Use Policy;*
- the Office of the Public Records Administrator *Public Records Policy 05: Disposition of Public Records;* and
- *State Agencies' Records Retention/Disposition Schedules*