RESCINDED ON 9/19/2012 – Replaced By OCPR Policy 12-01: Electronic Records Policy

Commission on Public Records
E-mail Retention Policy

and

Guidelines For Agencies
On Developing An Agency-Specific
E-mail Retention Policy

RESCINDED ON 9/19/2012 – Replaced By OCPR Policy 12-01: Electronic Records Policy

Commission on Public Records E-mail Retention Policy (5-01)

Purpose:
The purpose of this policy is to ensure that electronic mail is maintained by state agencies and county and local governmental entities in accordance with approved records retention policies, accepted record keeping practices and laws as required by IC 5-14-3-3, IC 5-14-3-7 and IC 5-15-5.1-10.

Policy:
E-mail is a public record
All e-mail conducted on state government computers is owned by the state of Indiana and is a public record. Indiana Code 5-14-3-2 defines a public record as:

> any writing, paper, report, study, map, photograph, book, card, tape recording, or other material that is created, received, retained, maintained or filed by or with a public agency and which is generated on paper, paper substitutes, photographic media, chemically based media, magnetic or machine readable media, electronically stored data, or any other material, regardless of form or characteristics.

The General Assembly essentially precludes any state agency or state employee from determining individually what is or is not a record: anything, on any medium and created for any governmental purpose, falls under the rubric of public records law. Consequently, all e-mail messages are public records and are subject to record retention requirements. For the purpose of satisfying public records laws, e-mail is defined as not only the messages sent and received by e-mail systems, but all transmission and receipt data as well.

Electronic Mail (E-mail) is not a record series for retention scheduling purposes. Rather, the retention of E-mail must be based on content, not media type. E-mail should be retained for the same duration as other records of similar content included in a given record series on an approved retention schedule.

Responsibilities:
All agencies are responsible for developing guidelines and procedures to manage e-mail messages as part of their overall record-keeping systems. Agencies must maintain their E-mail in a manner that complies with approved retention schedules and the records management practices already established for other media as required by law. If a record series cannot be identified, a record series should be developed and included on the agency's approved retention schedule. All agencies should communicate this policy to their employees and should take the steps necessary to ensure employee compliance with this policy.

All agencies are responsible for the electronic mail activities of their users. State agencies have the responsibility to ensure that state-provided e-mail services are used for internal and external communications which serve legitimate government functions and purposes. Managerial authority over electronic mail services should be defined, and user training programs provided which address electronic mail usage and policies. Agencies may consider providing additional restrictions and guidelines regarding the use of electronic mail within their local environments. In considering the need for additional restrictions and guidelines, each agency should take into account its particular needs, mission, available technology, level of staff training, geographic diversity, and organizational culture.

Although confidential and sensitive information should not be included in electronic mail communications unless proper, formalized security precautions have been established, certain electronic mail communications may be privileged or confidential. It is the responsibility of each state agency to protect confidential and sensitive information where intentional, inappropriate, or accidental disclosure of the information might expose the State or an individual to loss or harm.

________{end of Policy 5-01}_________

Guidelines For Agencies On Developing An Agency-Specific E-mail Retention Policy

Electronic mail or e-mail is an information transfer system utilizing computers for sending and receiving messages. For many state agencies and county and local government entities e-mail is used as an effective form of communication, in some instances replacing telephone calls and printed memos. Because e-mail is frequently used to conduct state government business, it is critical that records managers develop policies and procedures that comply with the Commission on Public Records' e-mail policy to ensure that records created or received on e-mail systems are managed according to Indiana's public records laws.

E-mail Policy Components

The components of an e-mail retention policy should include:

- Write confidentiality statement. Include provisions for maintaining confidentiality.
- Establish assignment of ownership. Clearly communicate that both the sender and the receiver should save e-mail records to document transactions and responsibilities completely. For example, if Person A sends an e-mail message to Person B with important information that affects agency policy, the transaction includes not only Person A's sending of the information, but Person B's receipt of the information.
- Determine records subject to retention. Guide staff members in determining which e-mail messages are records. Also, outline a procedure for grouping e-mails into records series, as well as a records retention schedule for each series.
- Provide document management. Include procedures for organizing, storing, maintaining, accessing, and disposing of e-mail records. Also, establish a procedure for documenting your e-mail records policy, including the software and hardware in use, specific procedures, training efforts, staff member responsibilities, and records retention schedules.
- Summarize responsibilities. Make clear the records management responsibilities of staff members and groups (e.g., departments, project teams, committees) as they engage in their daily work.
- Ensure that your policy meets the State Ethics Commission's "Limited Use of State Resources" policy and Information Technology Oversight Commission's policies "Computer Use Policy-ITP 00-8" and "Information Technology Security Use Policy- ITP 03-01".

Recommended Process for E-mail Policy Development

Use the following steps to guide you as you develop your e-mail records management policy:

1. Identify and organize key stakeholders in your organization.
2. Draft the policy and process with the input of key stakeholders.
3. Meet with key stakeholders, including individual staff members.
4. Finalize the policy with the input and support of key stakeholders.
5. Implement the policy technically by setting up and testing the procedures.
6. Train the staff members on the new procedures. (Training is especially important because you must rely on staff members to ensure the integrity of the procedures.)
7. Implement the policy for staff members on a planned schedule.

On an on-going basis, from initial development to future policy changes, document the development of your e-mail records management policy, the policy itself, and changes to the policy.

Key Issues to Consider

Agencies can use the questions below to begin the development of their e-mail management policy. Discussion of the questions below will help:

- Ensure that you meet your legal and operational requirements.
- Gather staff member input, support, and compliance with your e-mail management policy.
- Integrate your records management policy with your overall electronic records management strategy.
- Ensure that staff members manage e-mail records at the appropriate points of use.

Discussion Questions

- Which e-mail messages are records subject to retention?
- What is the appropriate records series and records retention schedule for each records series? How should e-mail records be organized for long-term storage and access (e.g., project, department, function)? How will we retrieve and dispose of e-mail on our chosen storage media?
- How should our e-mail retention strategy coordinate with our other records management procedures (e.g., store all project-related e-mail with the other project documentation)? What documentation do we need for our process?
- How should we implement the procedures technically and operationally? How can we plan our implementation so the policy is widely used and accepted, but causes minimal disruption to our daily operation?
- How can we ensure staff member compliance and understanding? What process is reasonable to ask staff members to comply with?
- How should we train staff members? How accountable should we make staff members for compliance?

Training for Staff Members

Staff members will need to be trained on how to answer legal and operational questions about e-mail. Your training and documentation material should set forth guidelines that staff members can follow to answer such questions in the course of their work. For example:

- Is this e-mail a record subject to retention? Is this e-mail message administrative or ministerial (e.g., "Thursday staff meeting to start an hour late." or "Let's do lunch")?
- Does this e-mail message have long-term significance (e.g., "New policy finalized.")? Does this e-mail message document a transaction or operations function (e.g., a process, a decision, or a discussion)?
- Is this e-mail record public or not-public (confidential) as set forth by FIPA or HIPAA?
- What metadata must be captured when the e-mail message is saved?
- Which record series does this e-mail record belong in?
- Should the complete e-mail record be saved, including attachments and group list names
- Could this e-mail message ever be required as evidence in a legal action?

Retention Guidelines

Records created with e-mail

Electronic mail systems can transmit a wide variety of information, so records created or received by e-mail will vary according to their content and function. Basically, the content and not the medium determines the treatment of the message. E-mail records, like other agency records, must be classified within the appropriate record retention schedule.

E-mail messages fall within three broad categories:
1. Transitory messages, including copies posted to several persons and casual and routine communications.
2. Public records with a less than permanent retention period.
3. Public records with a permanent or permanent/archival retention period.

Retention guidelines for each of these categories are as follows:

- Transitory messages-No retention requirement. Public officials and employees receiving such communications may delete them immediately.
- Less than Permanent-Follow retention period for equivalent hard copy records as specified in an approved retention schedule. The record must be in hard copy or electronic format, which can be retrieved and interpreted for the legal retention period. When there is a doubt about the ability to retrieve an electronic record over the life span of that record, the record may be printed out. .
- Permanent or Permanent/Archival-Retention may be in the form of a hard-copy printout or microfilm that meets 60 IAC 2. The information must be eye readable without interpretation. Questions concerning microfilm should be addressed to the Commission on Public Records, Micrographics Division.

State agencies are responsible for instructing their employees in determining which e-mail messages fall within the above categories, in using retention schedules and in securing approval for destruction. Depending upon the function of the public record being generated by e-mail, state agencies may take steps to institute procedures for routinely printing E-mail records, including all transmission and receipt data in the system, and filing the printouts in the normal course of business.

Determining e-mail retention periods
All e-mail should be kept for the retention period identified on either the state's general records retention schedule or an agency specific schedule. The Commission on Public Records, Records Management Division must be consulted when retention for specific e-mail cannot be determined. Records Management Division will assist agencies with amending their current retention schedule to include the questioned e-mail. The content of any e-mail determines how long the record must be maintained. Examples of e-mail message categories to consider are the following:

1. Containing information developed in preparing position papers, reports, and studies;
2. Reflecting official actions taken in the course of conducting agency business;
3. Conveying information on agency programs, policy decisions, and essential transactions;
4. Conveying statements of policy or the rationale for official decisions or actions;
5. Documenting oral exchanges, such as meetings or telephone conversations, during which policy was discussed of formulated or other agency activities were planned, discussed, or transacted;
6. E-mail calendars reflecting the daily appointments of officials conducting state business;
7. Distribution lists for state business mail.

Ephemeral correspondence that is determined to have insufficient value to warrant its preservation by the State of Indiana may be deleted upon receipt. Examples are:

1. listserve messages
2. personal messages not conveying state business
3. agency memos without legal, administrative, fiscal or historical value

Employees should be encouraged to delete this type of correspondence as soon as possible. Deletion will free valuable disk space and allow the user easier access to needed files by avoiding unnecessary clutter within individual e-mail accounts.

Documentation requirements
Agencies may be responsible for establishing the validity and accuracy of their electronic records in court. Legal admissibility will largely depend on the quality of the documentation available for the system in use and the care and preservation of the electronic records produced. In addition, agencies collecting information on citizens, particularly that of a personal nature, should be aware of the Fair Information Practices Act (FIPA), **IC**4-1-6-1, as it defines statutory requirements for documentation. Note that in it, "personal information" is generously defined as:

> any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual, including, but not limited to, his education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or his presence, registration, or membership in an organization or activity or admission to an institution.

"Personal," in this instance, is not the same as "confidential". Much of the information which falls under this rubric remains accessible to the public. The intent of the law is to minimize the potential for the abuse of such information, confidential or not, by establishing certain guidelines for the collection, verification and dissemination of these records.

Records that fall within FIPA and federal HIPAA regulations
Because of FIPA and HIPAA, the importance of documenting procedures for systems dealing with personal information cannot be overemphasized. For any record keeping system thorough documentation will reduce confusion, and serve to establish the reliability and authenticity of the records created.

Documentation files should identify system hardware and software, formalize file naming conventions, back-up and security procedures, identify the sources and uses of information, as well as their confidential or non-confidential status, and outline quality control procedures and storage requirements. Documentation should also cover employee training procedures and the verification of employee attendance at training sessions.

Preservation

Several issues should be addressed when developing an e-mail retention program. E-mail systems in different agencies have a wide range of capabilities and characteristics. In order to determine what will ensure the most accurate, complete, and practical method of managing records transmitted by e-mail, agencies need to develop procedures that fit their specific situations. Understanding the capabilities of an agency's e-mail system is a prerequisite to determining how the records will be identified, organized and stored. An agency's LAN administrator is the best reference for understanding agency e-mail software and can suggest possible options for e-mail retention.

Accessibility

Agency staffs need to be aware that requests for access to non-confidential e-mail must be treated in the same manner as requests for other public records. The difficulty of retrieval is not a legitimate reason to deny access, so throughout the required retention period, it is in the interest of all concerned that e-mail records remain reasonably accessible.

Every effort should be made to systematically file e-mail records for convenient retrieval following standardized filing rules within the agency. Electronic mail files should be indexed in an organized and consistent pattern, and reflect the way the files will be used and referenced. For example, correspondence is often indexed by one or more of the following: the date sent or received, the name of the sender or recipient, and/or by subject. If the correspondence is related to a particular type of record, such as a personnel file, the primary index point will be what is used for that file. E-mail records maintained electronically have the potential advantage of supplying multiple access or index points.

Storage

Many computer systems have storage limitations, so that only 60 to 90 days of messages may be stored before operational problems are experienced. E-mail records that must be maintained in electronic format past that time can be downloaded to some other storage medium, such as hard disk, tape, diskette, optical disks or may be data warehoused. The retention period for the particular series is the best indicator of which storage media to choose.

Features of e-mail need to be retained

All features of e-mail systems including messages, calendars, directories, distribution lists and attachments such as word processing documents should be evaluated to identify documentary materials that satisfy the definition of a public record. For example, some electronic communication systems identify users by codes or abbreviated names and others identify the recipients of a communication only by the name of a distribution list. With these systems, directories or distribution lists must be retained to ensure identification of the sender and addressee(s) of messages that are records.

Security concerns

Security measures should be taken to protect e-mail records from unauthorized alterations or deletions. All e-mail subject to a retention schedule should be retained in read-only files. Agencies should regularly back up messages stored on-line to off-line media to guard against system failures or inadvertent erasures. Procedures for backing up electronic mail systems should be coordinated with the destruction of e-mail records so that no copies are maintained after the retention period has ended.

Locating retention and disposition information

The state's general retention schedule is printed in the Indiana Commission on Public Records' Records Coordinator's Handbook. The most current version is available either from the ICPR's Records Management Division or from ICPR's web page at: http://www.in.gov/icpr/2767.htm. Each agency has a specific retention schedule covering the unique records it produces.

Schedule copies are available from the agency records coordinator, ICPR's Records Management Division or ICPR's webpage at: http://www.in.gov/serv/icpr_retention
Agency records, including e-mail records, may not be deleted or otherwise destroyed without the authority of an approved records retention schedule describing the records and their disposition.

E-mail destruction

All e-mail must be disposed of in a manner that ensures protection of any sensitive, proprietary or confidential information. Magnetic recording media previously used for electronic records containing sensitive, proprietary or confidential information is not to be reused if the previously recorded information can be compromised in any way by reuse.

Ensure that employees are aware of e-mail retention

Agencies are responsible for ensuring that employees are familiar with the legal requirements for creation, maintenance, and disposition of records on e-mail systems. Because records may be created or received via an e-mail system, each agency using electronic mail should provide records management training and guidance for employees that includes criteria for determining which e-mail messages must be retained. Records management officers and records custodians should emphasize to users that electronic mail is a public record subject to retention. As such, standards of personal and professional courtesy and conduct should be defined.

As public employees, everyone has an obligation to apply the appropriate retention to e-mail sent and received and to provide access to e-mail in compliance with public records law. For more detailed information, agency managers should attend the "Information and Records Management Training" offered by the Commission on Public Records through the Department of Personnel's Management Institute.