CITY OF MILWAUKEE
CITY INFORMATION MANAGEMENT COMMITTEE
POLICY FOR RETENTION OF ELECTRONIC MAIL RECORDS

This policy explains the requirements for the appropriate methods of retention, disposition, and management of electronic mail resources as required under applicable Wisconsin state law.

I. Scope

Employees of all city agencies, including part-time and temporary workers, volunteers, interns, contractors, elected officials and all others who have been granted access to, who use or administer the electronic mail resources of a city agency, or transact public business via e-mail on behalf of a city agency are covered by this policy and are required to comply with its guidelines and procedures.

II. Definitions

Electronic Mail Resources refer to systems, networks, equipment, software, and processes that are used to create, receive, transmit, and store messages, information, and other documents relating to the conduct of public business of a city agency. These resources include "e-mail" messages as well as other electronic documents created or received and any attachments transmitted with the electronic message. When an individual conducts public business using a privately owned computer or e-mail provider, that portion of the e-mail message (and attachments) that carry public records is included in this definition.

Users refer to all individuals, groups, or organizations authorized by a city agency to access, use or administer its electronic mail resources.

End Users include originators and recipients of e-mail who must retain the information as part of their public duties.

City Agency includes all city departments and divisions, boards, commissions, committees, subcommittees, and all other city governmental bodies created by law, ordinance, rule or order.

Metadata. Metadata describes data as it relates to e-mail. Metadata may includes descriptors such as who received the message, date the message was created, sent, opened, edited, etc.

End User Device includes the variety of devices that can communicate via e-mail including, but not limited to, desktops, laptops and other mobile computing devices such as palmtops, personal digital assistants (PDA's), and smart phones. ,

Public Records includes all documents, pictures, maps, messages, charts, electronically formatted documents or other documentary materials which are recorded or preserved

regardless of physical form or characteristics, which have been created or are being kept by a city agency or user that relate to the conduct of public business.

Public records do not include, for example:

- Requests to schedule appointments, automatic appointment notifications.
- Electronic professional newsletters, communications from professional organizations.
- Duplicate copies of materials where the originals are in the custody of the same City agency and the duplicates would only be maintained for convenience or reference and for no other substantive purpose.
- Materials in possession of a user or city agency, which are available for sale, or which are available for inspection at a public library.
- Notices or invitations received by a city agency that were not solicited by the agency and that are not related to any official action taken, proposed or considered by the city.
- Drafts, notes, preliminary computations and like materials prepared for the originator's personal use or prepared by the originator in the name of a person for whom the originator is working; and, materials which are purely the personal property of the user that have no relation to his or her office or governmental duties.
- Materials to which access is limited by copyright, patent, or bequest.
- Advertisements.

III. Requirements for Retention, Disposition and Management of E-mail Public Records

A. Retention and Disposition of E-mail Public Records

(1) Users shall save for retention all electronic messages and attachments that constitute part of a public record as defined above, according to the relevant record retention schedule.

(2) Users shall save their electronic messages in compliance with the City agency records retention schedule that relate to the complete content of the message, including attachments and metadata. These are the same schedules used for retention of records in other media.

(3) Users shall not delete, allow, or cause to be deleted without an approved record retention schedule any electronic messages that constitute part of a

public record. When there is a pending public records request or a likelihood of litigation, audit, or investigation, regularly scheduled retention schedules must be suspended until the risk is settled or until legal advice has been obtained concerning disposition.

(4) An e-mail record includes:

(a) The structure of the message;

Structure includes the physical appearance of the information in the message including, but not limited to, headings, body, form and signature blocks.

(b) The content of the message;

Content includes the subject matter information carried within the message.

(c) Its related contextual information;

Contextual information indicates the relationship of the message to the programmatic, business and technical environment and includes, but is not limited to, elements such as the origin of the record, the date and time created, the network paths it has moved along and the record series to which it belongs, and other metadata.

(d) Attachments.

Attachments are self-contained document files that are attached to an electronic message. Attachments should be managed the same way as other records and e-mails. If the electronic message is a record, the attachments must be retained with it. Retention must be for whichever is the longest retention period; either that for the e-mail content or that for any of its attachments.

(e) E-Mail Threads.

An e-mail thread, or string, is an e-mail conversation on a similar subject.

(5) Confidentiality and Security. Applicable confidentiality and security requirements for the content of messages and attachments must be maintained throughout the life of the record.

(6) Drafts are generally not retained as part of the record as they may not reflect the final authorized position of the agency. Generally, drafts should be purged after the final version has been approved unless retention of drafts is required by the

agency. Records distributed in other City Departments or to agencies or individuals outside the City may loose their "draft" status. Contact the City Attorney's office if there is a question as to whether a record is a draft.

(7) Originals and Duplicates: For e-mails created and distributed within the same City agency, the record "original" is generally considered to be the one that is held by the creator of the message. All other copies within the City agency may be destroyed at will unless there is a legal or business requirement for the recipient to document the business activity. E-mail becomes a record to the recipients if the recipient takes action or makes decisions based upon its content, it constitutes part of a case file or other record series, it concerns government business, or if there are specific programmatic or legal requirements for the information to be retained.

For e-mails received from outside the agency and that are classified as public records, at least one addressee within the receiving agency must retain the e-mail as the receiving agency's "original."

If messages and attachments are edited and forwarded, then the forwarding person is considered to have a new "original" and is responsible for its retention. For Intra-city system notifications only the original notification need be kept by the creator of the message.

B. Management of E-Mail Public Records

(1) Appraisal and Classification

Those electronic messages that are classified as public records are subject to the agency's records retention schedule. Guidance for users on appraising and classifying electronic messages that are the official record may be found by contacting the City department or division's records coordinator.

(2) Preservation

(a) Preservation: Electronic messages preserved in an electronic format shall be maintained in a manner that assures their authenticity, reliability, and integrity. They must contain sufficient data about the creation, routing, and receipt of the message as well as other objects such as text files, embedded documents, images, or hyperlink references and other metadata. The record must be accessible in a usable manner throughout its lifecycle.

(b) Migration: When messages identified as agency records are to be migrated, they must be moved to a storage medium and format that protects the content, metadata, attachments, hyperlink references and proof of delivery receipt when applicable. A migration audit trail shall be maintained with the record.

(3) Storage

(a) Unnecessary electronic mail: Unnecessary electronic mail messages should be deleted by end users to avoid excess accumulation and demand for storage on electronic mail servers. Unnecessary e-mail includes those that are not a public record or required for continued efficient work effort by the end user.

(b) Business critical information: Electronic mail messages that are public records should be stored outside the desktop local drive or end user device and successfully backed up.

(c) Saved electronic mail messages: The approved record retention period for electronic mail messages is determined by the message content and the applicable category in approved records retention schedules.

(d) Backup: Backup of messages is used to allow recovery of lost or damaged e-mail resources and not as a means of record retention.

IV. Responsibilities

The City's Chief Information Officer shall develop appropriate guidelines and standards for use by City agencies in implementing this policy. City agency heads are responsible for ensuring that this policy is properly communicated, understood and implemented within their respective organizational units. They are also responsible for defining, approving, and implementing processes and procedures in their organizational units, and ensuring consistency with this policy, and guidelines and standards issued by the Chief Information Officer.

All users are responsible for complying with this policy and the associated guidelines provided by management.

V. Enforcement and Exception Handling

Failure to comply with this policy and associated guidelines and procedures may result in disciplinary actions or other penalties applicable by law. Requests for exceptions to this policy should be submitted to the CIMC through its executive secretary, the City's Chief Information Officer. Prior to official approval of any exception request, the individuals, groups, or organizations identified in the scope of this policy will continue to observe this policy.

93529:1052-2005-83