

GLENN A. GRANT, J.A.D.
Acting Administrative Director of the Courts

www.njcourts.gov • Phone: 609-376-3000 • Fax: 609-376-3002

Directive # 03-18

TO: Hon. Carmen Messano
Assignment Judges
Hon. Joseph M. Andresini
Presiding Judges – Civil, Criminal, Family, General Equity, Municipal
AOC Directors and Assistant Directors
Clerks of Court
Trial Court Administrators
Division Managers – All Divisions

FROM: Glenn A. Grant, J.A.D. 

SUBJ: Electronic Mail (email) Retention Policy and Destruction Protocol

DATE: May 29, 2018

As authorized by the Supreme Court, this Directive hereby establishes a seven-year retention period for all Judiciary electronic mail (e-mail). There are two limited categories of exemptions from the seven-year retention period: (1) those judges and employees who are on litigation hold, and (2) a limited list of judges and employees as approved by the Administrative Director of the Courts.

This Directive also promulgates the attached protocol establishing the criteria for the electronic destruction of Judiciary email by the Judiciary's Information Technology Office. The protocol sets forth six standards that collectively establish the minimum requirements for maintenance, retention and destruction of email to ensure compliance with other Judiciary policies, including Directive #03-01 ("Judiciary Records Management") and Directive #01-14 ("Electronic Records Management Guidelines").

The destruction protocol applies to all e-mail content produced, received, or stored by Judiciary employees during the course of official business. The Director of the Information Technology Office will manage e-mail records subject to the seven-year retention period centrally, via a vault or journaling system, and manage end-user e-mail boxes centrally with respect to disposition actions. Specifically, e-mail content stored in end-users' mailboxes that: (1) falls under the Judiciary retention schedule, (2) is not subject to litigation hold or

other approved exemption, (3) is seven years old or older, and (4) that has been authorized by the Clerk of the Superior Court for disposal, will be disposed of along with the centrally stored record copy versions.

To conform with disaster recovery and litigation hold requirements, the Judiciary established an enterprise archival system that maintains a copy of all emails sent to/from Judiciary user accounts. This program began the archival process in October 2009. It is estimated that tens of millions of emails over seven years old reside in both the archival system and in active mailboxes due to the previous lack of an email retention schedule and destruction protocol. Given the volume of emails subject to destruction, **the destruction protocol will be implemented on July 1, 2018** so as to provide time for judges and staff to save particular emails from among those emails eligible for destruction.

Technical staff at both the vicinage level and the central office will be provided with directions on how to save any emails as documents outside the mailbox. Those staff will share those directions with judges and staff. Documents saved in that manner will no longer be treated as official email communications. These documents may be stored in various document repositories (e.g., My Documents, OneDrive, SharePoint) and will be subject to the same practices as all other files in those folders when requests for discovery are made. We strongly recommend that users do not bulk copy emails from Outlook to a storage area. ITO will identify clusters of emails moved in bulk and work with Court Executives to remove unnecessary saved email clusters.

Questions or concerns regarding this Directive may be directed to Michelle M. Smith, Clerk of the Superior Court, at 609-815-2900 ext. 54200 or michelle.smith@njcourts.gov.

Attachment (Protocol)

c: Chief Justice Stuart Rabner
Associate Justices
Hon. Jack Sabatino, Deputy Presiding Judge for Administration
Steven D. Bonville, Chief of Staff
Meryl G. Nadler, Counsel to the Administrative Director
Nicole Langfitt, Deputy Counsel to the Administrative Director
Melaney S. Payne, Special Assistant
Ann Marie Fleury, Special Assistant
Jessica Lewis Kelly, Special Assistant

JUDICIARY PROTOCOL
FOR RETENTION AND DISPOSITION OF
ELECTRONIC MAIL (E-Mail)

Promulgated by Directive #03-18
May 29, 2018

I. Introduction

This document sets forth the guidelines for managing the general retention and disposition of electronic mail (e-mail) produced, received and/or stored by the Judiciary.

The policies and procedures reflected in these guidelines:

- Ensure the Judiciary's capacity to capture, retain, and dispose of e-mail messages and attachments in alignment with Directive #03-01, Judiciary Records Management; and Directive #01-14, Electronic Records Management Guidelines.
- Establish how long e-mail and attachments must be maintained, and how and when to dispose of the content in an orderly, documented and accountable manner.

Storage and operational efficiencies will result from timely disposition of e-mail and attachments in accordance with approved retention periods.

II. Scope

All Judiciary offices, divisions or units that use a system to transport e-mail messages and attachments from one computer user to another are required to implement and adhere to these guidelines. E-mail systems range from local systems that move messages to users within an office, division or unit over a local area network (LAN), to enterprise-wide systems that carry messages over a wide-area network (WAN), to systems that send and receive messages over the Internet.

Systems maintained by the Judiciary or by third-party service providers on behalf of any Judiciary office, division or unit on Judiciary premises or on the service provider's premises are subject to these guidelines.

All e-mail content produced, received and stored by Judiciary e-mail systems is within the scope of these guidelines. This applies to all of the elements of the content, including messages, attachments and system-produced information that describe the content (metadata). E-mail content from both presently operational and decommissioned systems is within the scope of the guidelines.

III. Authority

The Supreme Court, through its adoption of Rule 1:38 (“Public Access to Court Records and Administrative Records”), has recognized that both court records and administrative records constitute vital documentation of decisions made, policies promulgated and actions taken.

Rule 1:38-2 broadly defines a “court record” as including:

- (1) any information maintained by a court in any form in connection with a case or judicial proceeding, including but not limited to pleadings, motions, briefs and their respective attachments, evidentiary exhibits, indices, calendars, and dockets;
- (2) any order, judgment, opinion, or decree related to a judicial proceeding;
- (3) any official transcript or recording of a public judicial proceeding, in any form;
- (4) any information in a computerized case management system created or prepared by the court in connection with a case or judicial proceeding;
- (5) any record made or maintained by a Surrogate as a judicial officer.

Rule 1:38-4 broadly defines an “administrative record” as including “[a]ny information maintained in any form by the judiciary that is not associated with any particular case or judicial proceeding.” Since the Supreme Court has broadly defined judiciary records to include any and all information maintained by the Judiciary in any format, a system or application used to conduct either case management or administrative functions essentially contains and constitutes the court’s “record.”

The Supreme Court’s authority to manage Judiciary records is set forth in N.J.S.A. 2B:1-2 (“Preservation of Court Records”), which provides that “[t]he Supreme Court may adopt regulations governing the retention, copying and disposal of records and files of any court or court support office.” The regulation of records by the Court is governed by Rule 1:32-2 (“Books and Records”) and Rule 1:32-2A (“Electronic Court Systems, Electronic Records, Electronic Signatures”). These Rules are broad in scope in order to address records in any medium.

Given the definition above, e-mail, attachments and associated metadata fall within the scope of records and files of any court or court support office.

Rule 1:32-2 (Books and Records)

- (a) Recordkeeping by Clerk. The clerks of all courts shall keep such books and records and may microfilm or electronically retain or destroy the same as the Administrative Director of the Courts with the approval of the Chief Justice may prescribe.

(b) Municipal Court Books and Records. Judges or presiding judges of the municipal court shall be responsible for the keeping of such prescribed books and records for the municipal courts.

(c) Retention Schedules and Purging Lists. Retention schedules identifying the length of time court records must be kept prior to destruction and purging lists identifying documents to be removed from case files before storage or replication shall be adopted by administrative directive. For purpose of this rule, “purging” means the removal and destruction of documents in the case file which have no legal, administrative or historical value.

(d) Reproduction of Original as Evidence. In the event of any destruction or other disposition of court records pursuant to this rule, the photographic or electronic reproduction or image of the original or a certified copy of same shall be receivable in evidence in any court or proceeding and shall have the same force and effect as though the original public record had been there produced and proved.

Rule 1:32-2A. (Electronic Court Systems, Electronic Records, Electronic Signatures)

(a) Authorization of Electronic Court Systems. The Administrative Director of the Courts, with the approval of the Chief Justice, may develop and implement electronic court systems, including applications or systems for the purpose of electronic filing, electronic record keeping, or electronic indexing of data and documents.

(b) Force and Effect of Data and Documents Submitted or Maintained Electronically. Data and documents, whether originating in paper or digital form, submitted electronically to the clerks of court or maintained electronically by the clerks of court in a system or application authorized pursuant to this rule shall have the same force and effect as data and documents maintained by the clerks of court in paper form.

(c) Electronic Signatures. Where an electronic system or application has been authorized pursuant to this rule, and where the system or application is secured by an authentication method in accordance with the protocols established and approved by the Administrative Director of the Courts, an electronic signature shall have the same force and effect as an original handwritten signature. Once submitted to the clerk of court, an electronically signed document shall not be deleted or altered in any manner without court order for good cause shown.

IV. FRAMEWORK

The framework consists of six foundational elements (Section IV.A) and an aligned e-mail retention and disposition program (Section IV.B).

The retention and disposition program is based on a broad seven-year retention period for

most common types of e-mail records, except those on litigation hold, including internal and external correspondence, and a limited number of judges and staff, as approved by the Administrative Director.

A. Foundational Elements

The Information Technology Office and, where necessary, other Judiciary offices, divisions and units must implement, or otherwise have in place, the following foundational elements no later than 180 days following the promulgation date of this protocol. In addition, each judge and Judiciary employee must complete an annual policy acknowledgment certifying both receipt of and understanding of this protocol.

1. Acceptable use policies covering e-mail and the Internet.

Acceptable use policies describe the permissible uses of e-mail and the Internet (a resource aligned with e-mail usage). Employees' responsibility with respect to these permitted uses, and the potential sanctions for non-compliance are specified in the "Judiciary Internet Access and Use Policy" and the "Statewide Judiciary E-Mail Template Policy," which can be found under "Information Technology Policies" on the Judiciary Infonet.

Action Step: Ensure that each judge/employee receives and reviews these policies.

2. Litigation hold process.

A legal or litigation hold is a communication issued as a result of current or reasonably anticipated litigation, audit, government investigation, or other such matter that suspends the normal destruction or other disposition of particular records. Legal holds may encompass procedures affecting data that is accessible as well as data that is not readily accessible. A legal hold directs recipients to identify and locate records pertaining to the matter or subject of the legal hold and is an order to preserve all such records, regardless of form, related to the legal hold. The litigation hold process encompasses the technical and operational requirements for identification, preservation, and ultimately, production and presentation of relevant records.

Action Step: Ensure that all e-mail system administrators, records custodians and legal advisers are aware of and can respond effectively to litigation hold requests.

3. Response for record request/tracking process.

As noted, the Supreme Court, by its adoption of Rule 1:38 (“Public Access to Court Records and Administrative Records”), has recognized that both court and administrative records constitute vital documentation of decisions made, policies promulgated and actions taken. Because e-mail messages and attachments serve to document organizational functions, policies, decisions, procedures, operations or other official activities, all such content meets the definition of a Judiciary record under Rule 1:38. The content must, therefore, be available to the public for the length of its designated retention period, unless it is exempt from public disclosure consistent with one of the exceptions enumerated in Rule 1:38 or by specific court order.

Action Step: Ensure that all e-mail system administrators, records custodians and legal advisers are aware of Judiciary policy regarding public access to records and can respond appropriately to such requests.

4. E-mail vaulting/journaling platform combined with central management of end-user e-mail boxes.

Institute an e-mail vaulting/journaling platform that makes exact copies of all content flowing from/to individual e-mail mailboxes, across the Judiciary, to a separate, secure and centrally controlled repository that allows authorized Judiciary end-users to access their vaulted/journaled content. Also, ensure that the platform can manage all end-user mailbox content from a centralized console. In this context, centralized management includes the ability to copy, move, transfer, and delete end-user e-mail boxes or selected content from the e-boxes by an authorized system administrator.

Action Step: The Judiciary Enterprise Vault and Microsoft Exchange Messaging system – which the Information Technology Office (ITO) has implemented with an on premise version and which will soon be moving to cloud-based versions – will include the requisite vaulting/journaling and central management features.

5. System security.

Develop and document technical, procedural and physical controls that will be applied:

- (a) To prevent unauthorized or unintended access, use, distribution, modification, or destruction of e-mail records; and,
- (b) To ensure message authenticity, integrity and retrievability/usability over time. Generally, this is the responsibility of information officers and, if applicable, any third-party service providers.

Action Step: The Judiciary Enterprise Vault and Microsoft Exchange Messaging system – which the Information Technology Office (ITO) has implemented with an on premise version and which will soon be moving to cloud-based versions – will

include the requisite system security.

6. E-mail back-up/recovery and disaster recovery/continuity of operations programs.

Develop, implement, and document a back-up and recovery program for both real time e-mail content and archive content, and institute a fail-over disaster recovery/continuity of operations capability for the e-mail system.

Action Step: The Judiciary Enterprise Vault and Microsoft Exchange Messaging system – which the Information Technology Office (ITO) has implemented with an on premise version and which will soon be moving to cloud-based versions – will include these requisite features.

NOTES ON BEST PRACTICES: End-user awareness and training programs will help the Judiciary achieve success with regard to e-mail retention and disposition.

The Judiciary Enterprise Vault and Microsoft Exchange Messaging system, which features centralized management of e-mail content, will address the general retention and disposition of e-mail associated with employees who separate from the Judiciary.

E-mail retention and disposition requirements apply to all e-mail systems and content — current and any legacy systems/content. Therefore, if the Judiciary is updating to a new e-mail system, it should have e-mail from the legacy system either migrated to and managed by the replacement system's archive/journal facility, or manage the legacy content by storing it on accessible, readable and secure media for the length of the latest retention period for any record series involved.

The Judiciary should also direct its internal and/or third-party audit teams to include checks for compliance with general records management requirements, including this framework.

B. Retention and Disposition Requirements

Once the foundational elements are in place, the Director of the Information Technology Office shall implement the Judiciary E-mail records retention and disposition requirements, specified below, for all Judiciary offices, divisions and units. These requirements are based on, and designed to operate in conjunction with basic records management program concepts and practices as specified by Directive #03-01, Judiciary Records Management, and Directive #01-14, Electronic Records Management Guidelines.

All e-mail content produced, received and/or stored by Judiciary employees during the course of official business is considered a court record and/or administrative record. This status applies to all of the elements of the content, including messages, attachments, and system-produced

information that describes the content (metadata). As such, e-mail content is subject to disclosure/retention under the provisions of Rule 1:38 (“Public Access to Court Records and Administrative Records”) and Directive #03-01 (“Judiciary Records Management”).

E-mail content is available for public inspection in accordance with Rule 1:38 and is subject to records retention and disposition requirements set forth in Directive #03-01.

- (1) Retention Requirement:** Judiciary e-mail records shall be retained for a period of seven (7) years from the date of creation or receipt, unless the e-mail is subject to litigation hold or there is an approved exemption. E-mail that is subject to litigation hold must be retained while on hold. Retention means that any record series that must be kept must be maintained in the e-mail system, and content from the e-mail system may be used as the source for record copies of such record series. (A record series is a group of identical or related records that are normally filed together and evaluated as a unit to determine how long it should be maintained. Examples include internal and external correspondence, subject files, legal files and most fiscal and personnel records. Record copies are the original or official versions of records.) The Office of the Superior Court Clerk will include a record series used to identify e-mail content subject to the Judiciary retention period in a conforming retention schedule for the Information Technology Office. This protocol will be promulgated as a Directive. The retention period also will be reflected in a subsequent more detailed retention schedule.
- (2) Disposal Requirements:** The Director of the Information Technology Office will manage e-mail records subject to the seven-year retention period, centrally, via a vault or journaling system and manage end-user e-mail boxes centrally with respect to disposition actions. Specifically, e-mail content stored in end-users’ mailboxes that: (1) falls within the Judiciary retention schedule, (2) is not subject to a litigation hold, (3) is seven years old or older, and (4) that has been authorized by the Clerk of the Superior Court for disposal, will be disposed of along with the centrally stored record copy versions.
- (3) Implementation of the Judiciary e-mail disposition process.** The Director of the Information Technology Office shall implement the e-mail disposition process by executing the steps below at least once per calendar year (as applicable with ITO and/or by third-party service providers).

 - (a) Identify vaulted/journaled and end-user e-mail content that is eligible for disposition (i.e., all e-mail, not on litigation hold, that has aged to seven (7) years or as which there is an express exemption).
 - (b) Document the impending disposition action by submitting a blanket Request and Authorization for Records Disposal Form to the Clerk of the Superior Court to cover the entire calendar year.

- (c) The Superior Court Clerk shall review the disposal request for completeness and enter the date of authorization and the authorization number. The Clerk will approve, disapprove or amend the request for authorization based on the promulgated Directive and/or adopted retention schedule.
- (d) If approved, the Superior Court Clerk will sign the authorization request form. If not approved, the request will be returned to the Director of the Information Technology Office with an explanation of errors to be corrected.
- (e) When approved, the Clerk of the Superior Court files the original and returns a signed copy to the Director of the Information Technology Office.
- (f) The Director of the Information Technology Office shall examine the returned copy for any changes or omissions.
- (g) Upon approval by the Clerk of the Superior Court, the Director of the Information Technology Office shall segregate and securely delete the aged e-mail content (from central storage and end-users' mailboxes).
- (h) Deletion must be performed in a manner that ensures as much as practicable that any information that is confidential or exempt from disclosure, including proprietary or security information, cannot be read, reconstructed or reused.
- (i) In addition, the Director of the Information Technology Office must ensure an audit tracking that includes the date and time of the deletion/purging.
- (j) Once deletion has taken place as specified above, the Director of the Information Technology Office shall provide a report to the Clerk of the Superior Court that the e-mail content and related data (including all versions) were deleted as specified above.
- (k) The Director of the Information Technology Office will provide the Administrative Director of the Courts with a yearly implementation plan discussing the historical configuration steps in place to meet the policy.