

Information Technology Standards

Email Archive Storage

IT Standard Issued: [Date]
Supersedes: New Standard

Responsible Executive: HSC CIO

Responsible Office: HSC IT

Contact: To report violations of this standard, please call HSC user support (272-1694) or UNMH user support at 272-DATA.

Summary of Standard: This standard addresses the retention and storage of email messages at the University of New Mexico Health Sciences Center (UNM HSC), including UNM Hospitals. This standard creates a structured approach to how email is preserved, how long it is retained, and how it is stored. It describes the organization of a central archive for email retention and outlines a process which:

- Enables users to access their archived email in a consistent and reliable way;
- Allows the institution to access email more easily for purposes of adherence to best practices, record keeping, and legal and regulatory compliance; and
- Works with information technology storage systems to create an archive that is sustainable.

This approach will benefit users by assuring that important email messages older than 180 days will be retained and handled in a consistent manner. This standard will assure that business decisions commonly carried out through email can be more effectively reconstructed to validate and defend the decision making processes when necessary. Additionally, by having a consistent and documented e-mail retention and deletion standard, legal and regulatory compliance requirements will be met.

Users are reminded that communications and other documents made by means of University computing resources are generally subject to New Mexico's Inspection of Public Records Act to the same extent as they would be if made on paper, per the UNM Acceptable Computer Use Policy (2500).

Glossary:

Email Archive – Storage located separately from an individual user's active email system into which copies of email and related data such as attachments are collected. The archive supports eDiscovery, regulatory compliance, and data protection. The archive optimizes access times and storage requirements, which are imperative in reducing legal and regulatory liabilities and data storage costs.

eDiscovery – Electronic discovery (also called e-discovery or ediscovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

Regulatory Compliance – Refers to systems or departments at UNM which ensure that personnel are aware of and take steps to comply with relevant laws and regulations.

Active Email Account - When a user is logged on to the email system accessing their active or current account, as opposed to accessing read-only archived messages stored outside the live email.

Who is Affected by this Standard: All salud GroupWise email users.

Resources:

Novell GroupWise accounts
Reliable, high-capacity and high speed servers to house centralized email storage
Messaging Architects M+ Archiving product

Why We Have this Standard: Email is a primary source of institutional documentation which often contains crucial information not documented elsewhere. Email needs to be retained in a way that meets institutional and individual user needs and is compatible with storage capabilities. This document outlines standards for using a centralized storage method for retaining email which will make email archives more reliable and accessible to users, meet institutional legal requirements for ediscovery, and make better use of network systems.

Responsibilities: UNM HSC employees are responsible for reading this standard and understanding how email archiving works as outlined in this document. UNM HSC managers and supervisors are responsible for making their

employees aware of this standard and for communicating to their employees the importance of understanding the email storage and searching capabilities described in this document.

I. Standards:

Email messages older than 180 days in a user's active salud GroupWise account (either sent or received) will be copied to and stored in the central archive system. Archived messages will be retained according to the following standards:

1. Email older than 180 days that has been copied to the central archive from the user's active email account:
 - a. Messages in the central archive cannot be modified in any way.
 - b. Once email has been copied to the central archive it will remain in the user's active account for an additional 60 days before being purged from the active system; it will then only be accessible to through the central archive.
2. All email retained within the central archive will be subject to the following deletion schedule unless protected with a legal or administrative hold:
 - a. Trash items copied to the central archive will be permanently deleted after 30 days.
 - b. Junk folder items (see below for more information on Junk Mail handling) in the central archive will be permanently deleted after 90 days.
 - c. All other email within the central archive will be permanently deleted after 3 years.
3. Junk Email Handling
 - a. UNM HSC employees are encouraged to use the Junk Mail feature in GroupWise. Enabling this feature will keep low priority emails from cluttering the central archive. When using the Junk Mail feature, all incoming email where the sender is not already listed in the user's system address books (the Main GroupWise and Frequent Contacts address books) will be placed in the user's Junk Mail Folder. The user's email settings should ensure that items in the Junk Mail folder are deleted within 30 days.
 - b. To prevent trusted email from continuing to be sent to the Junk Folder, users should add the appropriate sender addresses to their email Trust List or Frequent Contacts.

II. Additional Requirements:

1. Access to the central archive
 - a. Individual user access to the central email archive storage will only be through the GroupWise web access application.
 - b. Full access to the central archive for e-discovery purposes will be highly restricted and must be approved in advance by the Executive Vice President for Health Sciences.
 - c. Access to the archive system for maintenance purposes will be strictly limited to authorized personnel.
 - d. All access to the central archive will be logged and audited.
2. Local copies of archived messages
 - a. Local archives will be disabled by default for new users. Users who want to maintain local backup copies of email can run their full GroupWise client in "caching mode" and request an exception to allow local archiving.
3. Storage management and recovery
 - a. Messages with attachments over 250MB will be blocked (the current size limit for messages received from outside the salud system is 100MB).
 - b. Total on-line mailbox storage is limited to 2GB.
 - c. Backup tapes will be made for disaster recovery purposes and will be retained as long as appropriate to ensure effective disaster recovery (30 to 90 days).
4. Record Keeping
 - a. The central email archive is not an official records repository. Records in the archive are to be considered working copies. Official records should be maintained within the proper department or enterprise resource. The official UNM/HSC or UNMH records manager may amend this standard as needed to address record keeping issues. All changes to the standard for accessing, copying or placing holds on records in the archive must be approved by the EVP or an appointed representative.
5. Email Holds
 - a. Users can request an email hold for any reason. When an email hold is placed on an account all email will be captured and retained until the hold is released.
 - b. Approval of an email hold is subject to resource availability.
 - c. Once a hold has been placed on an account messages are copied to the archive after 2 weeks. At that point the status of the message will be frozen in the email archive.
 - d. Involuntary holds may be placed on an account for business or legal reasons with the approval of the EVP or the legal office.

Exemptions and Exceptions: Requests for exemptions to this standard may only be granted under special circumstances. Any requests must be submitted in writing to the Executive Vice President for Health Sciences. Exemptions will be permitted only upon receipt of written approval from the Executive Vice President for Health Sciences. HSC IT Security Office will retain documentation of approved exemptions and will review them on an annual basis.

Enforcement: Suspected or known violations of this standard will be reported to the appropriate University officials, and may result in:

- Loss of individual computing privileges
- Accountability for conduct under any applicable University or campus policies, procedures, or collective bargaining agreements, including disciplinary action
- Disconnection of non-compliant systems from the UNM/HSC network

Suspected or known violations of University regulations and/or State and Federal law will be processed by the appropriate University authorities and/or law enforcement agencies.

Website Address for this Standard: <http://hsc.unm.edu/library/kmit/policies.shtml>

Related Documents: UNM Business Policy 2300 "Inspection of Public Records"
UNM Business Policy 3210 "Recruitment and Hiring"
UNM Business Policy 3710 "Personnel Information Disclosure Policy"

Contact information:

For information on this policy, please contact:

HSC CIO

Holly Shipp Buchanan, EdD
HSC Chief Information Officer
272-2548

UNMH CIO

Ron Margolis
Chief Information Officer
272-2168

Security Officer

Barney Metzner
HSC IT Security Officer
MSC09-5100
272-1696

To report suspected non-compliance activities to a corporate compliance officer:

UNM Hospitals 272-8761
UNM Medical Group 272-6036
SOM Office of Research 272-1887
HSC Compliance Hotline (anonymous) 1-888-899-6092
HSC Legal Department 272-2463
UNMH Security Dispatch 272-2160