The email retention subcommittee, a working group of the Information Technology Advisory Committee, has compiled a set of recommendations to guide information technology professionals in developing protocols for effective email retention. Effective protocols governing email retention balance competing user, legal, and technological interests. Ideally, these protocols should reduce risk to the university, comply with legal mandates, and create an effectively managed email infrastructure while providing convenience for our email users.

An overriding consideration in email retention protocols is the applicability of record retention policies as they relate to email. Email messages can be classified as transitory information (state records of limited value), convenience copies (no retention requirement), or state records that are subject to document retention policies. It is beyond the responsibility of information technology (IT) professionals to determine the status of an email message without guidance from the email sender or recipient. Therefore, document owners (senders and receivers) have an affirmative duty to take some form of action to delineate email as a state record subject to retention. IT administration shall determine in consultation with their users what form this standardized action will take. Units shall maintain a system to manage email messages subject to retention including; storage, review and process of destruction.

Retention of email messages beyond what is required by applicable rules and laws incurs risk to the individual, unit and university. Therefore, it is recommended not to retain email beyond its utility unless required to by applicable rules and laws. Although individuals may have a desire to maintain email beyond this scope for a variety of reasons, unit heads should be made aware that such practice incurs risk and should be weighed accordingly.
The use of email data backups is required by numerous rules and laws. However, data backups are intended and designed for disaster recovery purposes, not document retention. Restoration of email data from backups is considered forensic recovery and is not subject to Texas Public Information Act (TPIA) requests. Offline email storage files maintained and/or stored by the user are subject to TPIA requests as well. Moving email messages to offline storage does not reduce legal risk. Therefore, users should delete both online and offline messages that are not subject to retention schedules.

The email retention subcommittee recommends the following specific practices:

- Users should take some form of affirmative action to retain email messages beyond these limits.
- Retained email messages should be reviewed on a routine basis for destruction (as applicable)
- The deleted items folder should be automatically emptied at the close of each email session
- All sent items older than 30 days should be automatically deleted
- All junk mail items older than 30 days should be automatically deleted
- All inbox items older than 30 days should be automatically deleted
- The deleted/recovery time period (if applicable) for deleted email should be set to 1 day or less