https://www.umsystem.edu/ums/is/email-management-policy

Email Management Policy

Policy Number: 12006

Scope

This policy applies to all employees, students and other users of the University of Missouri's (UM) electronic mail (email) system and to all email sent from or received by the UM email system.

Purpose

To provide email services in support of the missions of the University while also reducing associated risks

Policy

University employees must use the University provided email account assigned to them when using email to conduct University teaching, learning research or other University-related business activities. Former employees, retirees, volunteers, consultants and others acting for or on behalf of the University may be eligible for a University email account. See Electronic Mail (Email) Use and Management Procedures for eligibility requirements.

Conditions and obligations for access to and use of the UM email services include:

1. Email is primarily a transactional communication tool and should not be used as a system of record or for long-term storage of files. When appropriate or necessary, emails and/or email attachments should be transitioned to appropriate electronic storage systems consistent with the University's record management policies.
2. The use of a University e-mail account for personal business should be limited as per CRR 110.00, UM Acceptable Use Policy.
3. The use of University passwords on non-University systems is strictly prohibited. This includes all personal online accounts/systems as well as work-related systems provided by non-UM entities.
4. Automatic forwarding of University email to a non-university email account is prohibited.
5. A device personal identification number (PIN) must be enabled in order to receive University email on a mobile device.
6. Email transmission of highly restrictive DCL4 data (SSNs, patient information, credit card numbers, etc.), as defined in the UM Data Classification System, to an external email account is strictly prohibited except through encrypted means.
7. Highly restrictive DCL4 data, as defined in the UM Data Classification System, shall not be stored in a University email account. Email messages and/or attachments containing DCL4 data must be deleted or moved to an appropriate storage location as soon as possible or within 30 days of receipt or transmission.
8. Emails will automatically be deleted from Inboxes, Sent Items, and Deleted Items after defined periods of time as documented in the *Electronic Mail Use and Management Procedures*. Emails moved to a subfolder will not be automatically deleted.
9. University email accounts will be deactivated and ultimately deleted when the individual to whom the account was assigned, is no longer approved to have UM email.
10. Supervisors must work with their employees, prior to their departure, to transfer any emails necessary for business continuity, particularly those that include University legal correspondence, proprietary or confidential information, compliance related correspondence and any records to an appropriate custodian prior to their last day of employment.

Procedures

The UM Office of Information Technology is responsible for publishing procedures related to the ongoing management this policy. Email management procedures will include but are not limited to email account retention, exception procedures and account deletion timelines.

Enforcement

Violation of this policy may result in a denial of access to University information technology resources and other appropriate disciplinary actions up to and including termination.

References

- Electronic Mail (Email) Use and Management Procedures
- University System Records Retention Schedule
- Data Classification System and Descriptions
- CRR 110.005 Acceptable Use Policy
- Policy 12001 on Management Use and Access of IT Resources
- Policy 12003 Information Security

Reviewed 2021-06-30