


ADMINISTRATIVE PROCEDURE

ITP-3

DIGITAL COMMUNICATIONS AND ACCOUNT MANAGEMENT

Number: ITP-3	Name: DIGITAL COMMUNICATIONS AND ACCOUNT MANAGEMENT
Purpose: The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy of information hold important implications for digital communications. The purpose of this procedure is to describe the boundaries, standards, and procedures that apply to the provision, use, regulation, administration, security and protection of the digital communications and account management systems in use by Marshall University.	
Responsible Unit: Information Technology	
Approved by: 	Approval Date: 5/20/2025

1. General

- 1.1 Scope: This procedure controls the provision and use of digital communications and account management systems within the Marshall University information technology environment.
- 1.2 Authority: Marshall University Chief Information Officer, as defined by ADMIN-20 Approval of Board of Governors Rules, University Policies and Administrative Procedures.
- 1.3 Passage Date: April 18, 2014
- 1.4 Effective Date: April 18, 2014
- 1.5 Revision Date: May 20, 2025
- 1.6 Controlling Over: Marshall University, Marshall University Research Corporation, Marshall University Foundation, Marshall University School of Medicine, and all Affiliates of Marshall University utilizing Marshall University Information Technology Services.
- 1.7 History: This procedure was previously approved as Email Protocol for Deceased Students, Faculty, Staff or Affiliate by the Information Technology Committee on 11/20/08. The original content has been preserved and expanded to include all procedures related to the electronic communications policy ITP –29. Clarifications were made to this procedure on 4/18/14. The policy was reviewed and updated to the Digital Communications and Account Management policy in 2025 with associated changes to the procedures for handling account types.

Previous IT procedures, ITP-5, Marshall University IT Identity, Access, Privilege, and Content Retention Procedure also merged into this policy.

2. User Account Creation

User accounts are created, as follows:

- Student accounts – created when an applicant is admitted to the University.
- Faculty and Staff accounts – created when they receive the Employee role in Banner.
- Affiliate accounts – created when Affiliate User Account requests are completed and approved.

3. User Account Identity

It will be the procedure of Marshall University to retain the assignment of the MUID identity to an individual permanently and not reuse the identifier even if a new identity assignment is made under this or other related policies. The MUNet ID and email address will be reserved and not reassigned to another individual. Under this policy the following provisions are made:

- When an identity is no longer in use it will be archived in either of two states:
 - Available for automatic reactivation (i.e., there is the possibility that a reactivation of this identity will be needed, e.g., returning student, faculty, staff etc.)
 - Not available for automatic reactivation (i.e., there is a reason that this reactivation would need administrative review, e.g., the death of an individual, a legal restriction, an administrative restriction, etc.)
 - If a new identity is assigned to an individual the original identity will be archived as not available (reserved) and only reassigned to the same individual.

4. User Roles and Privileges

It is the procedure of Marshall University that access to technology systems is assigned based upon an individual's role within the institution and change as roles change. Privileges are created, changed, or suspended based upon the role of an individual or an implicit request for elevated, expanded, or removed privileges, which must be approved by the appropriate authority. MUIT provides roles and privileges audit reports to faculty and staff supervisors annually, and it is the responsibility of the supervisors to ensure the appropriate roles and privileges for their direct reports of faculty and staff.

5. User Account Access Termination

User account access will be terminated by MUIT upon notification from Human Resources (HR). MUIT will provide the orderly termination and/or transition of account services resulting from a user termination date in Banner. This includes coordinating the removal of services and/or reassignment of access from the exiting user to the designated individuals within the department or business unit.

6. Email Account Management

6.1 Email Identity & Assignment

- 6.1.1 Students, faculty, staff and affiliates of Marshall University are eligible to be assigned one email identity/account in the marshall.edu domain, i.e., someone@marshall.edu.
- 6.1.2 Affiliated Personnel or Agents: It is recognized that work requirements for those who are affiliated with Marshall University, though not directly in its employment, may necessitate access to electronic services. Some categories of these agents are granted access by default. For those who do not fall within these categories, a request, including an explanation of the need, should be submitted to the IT Service Desk.

6.2 Email Retention and Backup

Email messages and appointments can be kept for as long as the User deems it necessary, if the space limit is not exceeded. If a User gets a message that they are out of space when sending or receiving mail, it is their responsibility to delete or archive mail. Deleted emails can be recovered by MUIT fourteen (14) days after deleting them from the mailbox's Recycle Bin.

6.2.1 What are the current email quotas/limits?

An email quota is the amount of email (including attachments) that a user can store. To manage available space and ensure equitable availability of computing resources, MUIT limits the amount of email an individual can store. For this reason, a mailbox should be regarded as only a temporary repository for email. Messages and attachments should be deleted if no longer needed. Email storage fluctuates based on availability provided by the university's email vendor and licensing.

6.2.2 What happens when a mailbox is over quota?

- Every night, the system checks mailbox size against mailbox quota and will generate a notification email when a mailbox is nearing the allotted quota.
- When a mailbox reaches or exceeds its allocated quota, email cannot be sent from that account.
- When a mailbox exceeds its allocated quota, email cannot be sent or received. Access to the mailbox is still allowed to perform housekeeping, but the ability to send or receive new messages will be suspended until the mailbox is within its allocated quota.
- The email systems manage quota calculations automatically; as contents in a mailbox are deleted and purged, the total amount of mail is compared against the mailbox quota and the ability to send and/or receive mail is automatically reset when appropriate.

- 6.3 Disposition of Email when the relationship with Marshall is interrupted. Individuals may leave the University to take other jobs, to transfer to another college, or simply to go on to other activities. Since such people often have no continuing relationship with the University, their email benefits may be reduced or terminated. The following situations describe what will happen to the marshall.edu email address starting July 1, 2025. For retired faculty and staff prior to July 1, 2025, users will continue to have access to their account unless there has been six months of user inactivity. At that time, the account will be deactivated, and the mailbox will be marked for deletion one month after deactivation.
- 6.3.1 Faculty/Staff
- 6.3.1.1 Faculty/Staff who are dismissed from their employment
- If a faculty or staff member is dismissed from the University 'for cause', access to email privileges will be terminated immediately upon the last day of employment. Once terminated, that person's mailbox will be marked for deletion one month after the termination date. An automated response will be generated in response to messages sent to the account indicating that mail should be directed elsewhere. New mail will not be delivered to the mailbox during this one-month period. Any requests to be provided with a copy of email should be directed to the Chief Human Resources Officer (CHRO) for staff or the University Provost for faculty. Upon request by the CHRO or Provost, other members of the University may be granted access to the mailbox to conduct the business of the University. Email address forwarding is not available.
- 6.3.1.2 Faculty/Staff who resign or retire voluntarily from employment.
- If a faculty or staff member voluntarily resigns or retires (without emeritus status) from the University, their access to email privileges will be terminated immediately upon the last day of employment. Resigning or retiring (without emeritus) faculty can request (with supervisor approval) to have continued access to their e-mail up to six months after their last day of employment. Extension of e-mail access is not available for resigning staff. Once a faculty or staff member has resigned or retired (without emeritus), that user's mailbox will be marked for deletion one month after the resignation/retirement date. An automated response will be generated in response to messages sent to the account indicating that mail should be directed elsewhere. New mail will not be delivered to the mailbox during this one-month period. Any requests to be provided with a copy of email should be directed to the Chief Human Resources Officer (CHRO) for staff or the University Provost for faculty. Upon request by the CHRO or Provost, other members of the University may be granted access to the mailbox to

conduct the business of the University. Email address forwarding is not available.

For adjunct faculty and other non-permanent employees, voluntary separation can be challenging to define. As a general guideline, an adjunct faculty member will be considered voluntarily separated if they have not been assigned a course within one academic year. However, exceptions may apply based on contractual obligations or anticipated future assignments.

- 6.3.1.3 Faculty/Staff who retire from the University with Emeritus status.
For faculty or staff who retire from Marshall University with Emeritus status may request continuation of their email and storage services. Upon approval of the Emeritus request by Human Resources, the account will be maintained in emeritus status.

6.3.2 Students

- 6.3.2.1 A student who is expelled.

If a student is expelled from the University 'for Cause', email access by the student will be terminated immediately upon receipt of notification by the Provost or Vice President of Student Affairs. The mailbox will be marked for deletion one month after the student's expulsion date. New mail will not be delivered to the mailbox during this one-month period. Any requests to be provided a copy of email should be directed to Provost or the Vice President of Student Affairs. Upon request by the Provost or Vice President of Student Affairs, University professional staff may be granted access to the mailbox. Email address forwarding is not available.

- 6.3.2.2 Students who leave before graduation.

Students who leave the university without completion of their degree or other program requirements may keep access to their email account if their leave status has been designated as "current". Once the leave status expires the email account will be marked for deletion after twenty-four (24) months. The student is responsible for making any needed copies of email during the period that there is still access to the mailbox. Upon request by the Provost or Vice President of Student Affairs, University professional staff may be granted access to a student's mailbox. Email address forwarding is not available.

- 6.3.2.3 Students who graduate or complete program requirements.

Students who complete their degree or other program requirements will maintain their email account for twenty-four (24) months from the last day of the semester where their degree requirements were completed. After twenty-four months, the email account will be marked for

deletion. The (former) student is responsible for making backup copies of email during the period in which there is access to the mailbox. Upon request by the Vice President of Student Affairs, University professional staff may be granted access to a student's mailbox. Email address forwarding is not available.

- 6.4 Email Address Blocking:
Marshall University Information Technology (MUIT) reserves the right to block email from harmful addresses, domains, or IP addresses of known sources of unsolicited commercial and bulk email.
- 6.5 Confidentiality of email:
Authorization for University personnel to monitor or access the electronic communications of individual faculty, staff, students, and affiliates will not be granted without written consent from the appropriate leadership authority (i.e., Student – Provost or Vice President of Student Affairs, Faculty –Provost, Employee – Human Resources, Affiliates – Executive Sponsor). Such authorization will require justification based on reasonable business needs or substantiated allegations of a violation of law or policy on the part of the employee or student. In conducting the retrieval of files or information, due respect should be accorded to confidential or personal information and legally protected files. Whenever possible, the user should be informed and asked to help with obtaining the business materials needed.
- 6.6 Group Email Accounts:
Requests for shared departmental accounts will be accommodated, but require the designation of an account holder, who will administer the addition, deletion, or modification of names within the account. The designated account holder of shared mailboxes and groups will be periodically queried for utilization and resources may be terminated if not actively utilized. Group accounts and maintenance can be requested through an IT Service Ticket.
- 6.7 Use of Departmental Email for External Communications
When engaging with external vendors, reporting data, or conducting official university business, faculty and staff should use a designated departmental email address rather than their individual university email.
- 6.8 Protocol for Student, Faculty, Staff and Affiliate Email upon Death
The procedure for account termination due to the death of a student, faculty, staff, or affiliates will follow the procedure as defined for any terminated student, faculty, or staff, or non-active student, as defined in this procedure. All access, forwards, and custom autoreply to requests must be documented in an IT Service Request.

6.9 Multiple relationships with the University:

Individuals may have more than one affiliation with the University. A faculty member may also be a former student, a staff member may be a student, a staff member may be a part-time faculty member, etc. A person with multiple roles will receive the account specifications that are associated with his/her primary role at the University.

6.10 Limits on use:

Email and network connectivity are provided as professional resources to assist faculty, staff, and students in fulfilling their academic goals and/or University business.

Each user is responsible for using the email systems in a professional, ethical, and lawful manner. In addition to unacceptable and inappropriate behavior included in the University Terms of Use Policy other violations include, but are not limited to:

- Forged Mail - It is a violation of this policy to forge an electronic mail signature or to make it appear as though it originated from a different person.
- Intimidation/Harassment - It is a violation of this policy to send/forward email that is obscene, harassing, abusive, or threatens an individual's safety. Known threats to personal safety will be reported to the University Police.
- Unauthorized Access - It is a violation of this policy to attempt to gain access to another person's email files regardless of whether the access was successful or whether the messages accessed involved personal information.
- Unlawful Activities - It is a violation of this policy to send/forward copyrighted materials electronically, and it is a federal offense. Other illegal use of emails will also be dealt with and/or reported to the proper authorities.
- Proprietary/Confidential Information - The unauthorized exchange of proprietary information or any other privileged, confidential sensitive information, without proper authorization, is a violation of this policy.
- Chain Letters/Junk email/SPAM - It is a violation of this policy to send chain letters, junk email, or any other type of widespread distribution of unsolicited email.
- Hoaxes - It is a violation of university policy to distribute an email hoax with the intention to mislead or trick others into believing/accepting/doing something.
- Viruses - It is a violation of this policy to knowingly transmit email messages containing a computer virus, worm, spyware, or any form of malware.

- Commercial Activities - It is a violation of this policy to use Marshall's email system for commercial activities or personal gain.
- Attachments - Attachments are any items added in addition to the original email being created. Attachments must also adhere to the restrictions stated above.
- Public Forum - Using communications as a public forum to broadcast religious or political beliefs is prohibited. This includes transmitting political and religious documents and signature lines with quotations that might be offensive to other political, religious, or non-religious individuals. This is in the interest of remaining fair and unbiased to all political and religious affiliations.
- Penalties for unacceptable behavior range from de-activation of the account (for minor first offenses) through university judicial action or referral to law enforcement authorities.

6.11 Email security and confidentiality:

Email transmission over the Internet is inherently insecure and subject to security breaches that include message interception, message alteration, and spoofing. Users of Marshall's email systems should not assume the confidentiality or integrity of any message that is sent or received via the Internet. Also, while the transmission and receipt of email messages is reliable, timely delivery of time-sensitive information cannot be guaranteed. Marshall University Information Technology (MUIT) encourages the use of e-mail encryption protections when sending data that is considered private or restricted.

6.12 Email privacy:

While the University respects the privacy of digital communications and makes every attempt to keep email messages secure, privacy is not guaranteed. Marshall University does not routinely monitor or access the content of email messages whether stored on university equipment or in transit on the University network. The content of electronic communications will not be accessed during the execution of systems support, network performance, and related security functions; but system administrators may access and disclose such contents when access and disclosure are necessary to protect the integrity of information technology resources, to ensure that these resources are equitably shared, to respond to health and safety emergencies, or to respond to subpoenas, court orders, or other valid forms of legal process. Where there is evidence of a criminal offense, the matter will be reported to Marshall's judicial systems and/or law enforcement. The University will cooperate with the justice system in the investigation of the alleged offense.

In addition, with appropriate authorization, the University will investigate complaints received from both internal and external sources about unacceptable

use of email that involves Marshall's email facilities and/or Marshall's computer network. Requests to access or disclose the content of email will be managed within the following guidelines:

If the email account belongs to a:	Then written permission must be obtained from:
Faculty Member,	Provost
Student	Vice President of Student Affairs or Provost
Staff Member (incl. student employees)	Chief Human Resources Officer
Alumni or Alumnae	Vice President for University Advancement
Affiliates	Executive Sponsors

All requests to access or disclose the content of email, including detailed information on why the request is being made, should be sent from the appropriate person authorized to the Chief Information Officer for processing. If the request is the result of a court order, then written permission from the above authorized person is not required.

6.13 Email policy dispute or interpretation:

The Chief Information Officer is charged with the responsibility to periodically review the policy and propose changes as needed through the shared governance process, as defined in ITP-1 Technology Governance and Procurement Review.