

## ADMINISTRATIVE PROCEDURE

### ITP-~~TBD~~3

#### DIGITAL COMMUNICATIONS AND ACCOUNT MANAGEMENT

Number: ITP- <del>TBD</del> 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 <del>electronic communications</del> digital communications. The purpose of this procedure is <del>to to implement the policies promulgated by the Marshall University Board of Governors specifically Policy No. IT-3 the Electronic Communications Policy, in which is described</del> the boundaries, standards, and procedures that apply to the provision, use, regulation, administration, security and protection of the <del>electronic-digital</del> communications <del>and account management</del> systems in use by Marshall University.	
Responsible Unit: Information Technology	
Approved by:	Approval Date:

#### 1. General

~~1.1~~ Scope: This procedure ~~is controlling over~~ controls the provision and use of ~~digitalelectronic~~ -communications ~~and account management~~ systems within the Marshall University information technology environment.

~~1.1~~  
~~1.1.2~~ Authority: ~~Marshall University Information Technology Council Marshall University Chief Information Officer, as defined by ADMIN-20 Approval of Board of Governors Rules, University Policies and Administrative Procedures.~~

~~1.2.1.3~~ Passage Date: April 18, 2014

~~1.3.1.4~~ Effective Date: April 18, 2014

~~1.4.1.5~~ Revision Date: ~~August 19, 2019~~ TBD

~~1.5.1.6~~ 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. Faculty, Staff, Students, and Affiliates of Marshall University~~

~~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 ~~-329~~. Clarifications were made to this procedure on 4/18/14. ~~The policy was reviewed~~

**Formatted:** Outline numbered + Level: 2 + Numbering  
Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned  
at: 0.5" + Indent at: 1"

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.

1.6

1.7 Related Policies: MUBOG IT 1 Information Technology Acceptable Use Policy, MUBOG IT 2 Information Security Policy, MUBOG IT 3 Electronic Communications Policy, MUBOG GA 14 Interim Business Record Policy

1.8 Related Procedures and Guidelines: MUITC : ITG 4 Guidelines for Data Classification, ITP 4 Mass Voice Mail Distribution Procedure, ITP 5 Information Systems Identity, Access, Privilege, and Content Retention Procedure.

## 2. Purpose

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy of information hold important implications for electronic communications. The purpose of this procedure is to implement the policies promulgated by the Marshall University Board of Governors specifically Policy No. IT 3 the Electronic Communications Policy, in which is described the boundaries, standards, and procedures that apply to the provision, use, regulation, administration, security and protection of the electronic communications systems in use by Marshall University.

## 3. Definitions

Refer to ITP 10 for Terms and Definitions.

## 4. Contents

<TABLE>

## 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:
  - o 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.)

Formatted: Indent: Left: 1", No bullets or numbering

Formatted: Indent: Left: 1", No bullets or numbering

- 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.

Formatted: Outline numbered + Level: 5 + Numbering  
Style: Bullet + Aligned at: 1.25" + Indent at: 1.5"

#### 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.

Formatted: Indent: Left: 0.5", No bullets or numbering

#### 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.

Formatted: Indent: Left: 0.5", No bullets or numbering

Formatted: Indent: Left: 0.5", No bullets or numbering

#### 5.6. Email Account Management Procedures

##### 5.1 Email General Information

Currently Marshall University Information Technology supports the following production Email systems:

- An internally operated Microsoft Exchange Mail environment for Faculty, Staff, and authorized Affiliates business related Email.
- A hosted Microsoft Exchange Mail (often referred to as live@edu, live.marshall.edu, or outlook.com) environment customized for Marshall University Students and also available for personal use by Faculty, Staff, and Affiliates.
- Also available in a pre-production/test environment is a similarly customized hosted Google Apps environment for Marshall University Students and Faculty, Staff, and Affiliates.

##### 5.2.6.1 Email Identity & Assignment

5.2.16.1.1 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. Other MU related email addresses are also assigned in the two hosted environments mentioned in 5.1 above, i.e., someone@live.marshall.edu or someone@gapps.marshall.edu. In the case of Student Email, the issued marshall.edu domain address is forwarded to the live.marshall.edu domain by default.

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 ~~affiliates-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.

### ~~5.3 Faculty, Staff, and Affiliates business email. Currently, Microsoft Exchange Mail:~~

#### ~~5.3.16.2 Email Mail Retention and Backup~~

~~Email systems literally have millions of messages throughout their database store. In order to accommodate system growth user quotas will be set.~~ Email messages and appointments can be kept for as long as the User deems it necessary, ~~as long as 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 messages or, if it is deemed necessary, that their quota be increased. Such requests may be denied. Denials may be appealed. Deleted emails can be recovered by MUIT fourteen (14) days after deleting them from the mailbox's Recycle Bin.~~ Email backup and retention will be based on a documented risk assessment, and is as follows:

- ~~• Full backups are done weekly. The retention period for these backups is four weeks~~
- ~~• Incremental backups are done daily. The retention period for these backups is four weeks.~~
- ~~• These backups are made for total system recovery and will be used to restore the system in the event of a catastrophic failure. Individual file or mailbox restorations are not possible.~~

#### ~~5.3.2 Data Purging and Record Retention~~

~~Unless a legal hold has been placed on an account, messages in University Email Accounts are automatically purged from folders as follows:~~

- ~~• Trash/Deleted Items—30 days~~
- ~~• Junk/Junk Email—30 days~~
- ~~• A legal hold will override any and all record retention schedules.~~

#### ~~5.3.36.2.1~~ What are the current email quotas/limits?

An email quota is the amount of email (including attachments) that a user can store ~~on the central email server~~. To manage available ~~disk~~ space and ensure equitable availability of computing resources, MUIT limits the amount of email an individual can ~~leave on the mail server store~~. For this

**Formatted:** Indent: Left: 1", No bullets or numbering

**Formatted**

**Formatted:** Default Paragraph Font, Font: 12 pt, No underline, Font color: Auto, Pattern: Clear

**Formatted:** Body Text, Indent: Left: 1.25", Right: 0.16", Space Before: 0 pt, Line spacing: Multiple 1.08 li, No bullets or numbering, Widow/Orphan control, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.57"

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, or more permanently stored on a hard drive, CD or other storage media. Current default quotas are documented in the IT services rate schedule.~~

~~Requests for increases may be considered on an "as needed" basis, provided that the usage supports the mission of the University and that all current best practices for mailbox management, as recommended by IT, are being followed. Increases in mail quota will not generally be granted if a mailbox is not actively maintained or if off-line storage, for long term archival purposes, is not being utilized.~~

#### ~~5.3.46.2.2~~ 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 ~~in order 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 ~~handle~~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.

Formatted: Indent: Left: 1.5", No bullets or numbering

#### ~~5.4~~ Student, alumni, and non-business faculty and staff Email: Currently, Office365 Mail or Google Mail.

##### ~~5.4.1~~ Mail Retention and Backup

~~Email literally has millions of messages throughout its database store. In order to accommodate system growth user quotas will be set. Email messages and appointments can be kept for as long as the User deems it necessary as long as 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 messages.~~

Live Mail backup and retention is determined by Microsoft and along with other information is documented at <http://help.outlook.com>.

#### 5.4.2 What are the current email quotas/limits?

An email quota is the amount of email (including attachments) that a user can store on the central email server. To manage available disk space and ensure equitable availability of computing resources, IT limits the amount of email an individual can leave on the mail server. 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 or more permanently stored on a hard drive, CD or other storage media. Current default quotas are documented in the IT services rate schedule.

#### 5.4.3 What happens when a mailbox is over quota?

When a Live Mail mailbox reaches its quota, it will no longer receive email or store sent mail. Access to the mailbox is still allowed in order 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 handle 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.

#### 5.5 Email backup

Marshall's Exchange system is backed up on a nightly basis strictly as a disaster recovery resource in the event of a hardware, software, or facility failure. User files and folders are not backed up individually, and the IT staff cannot accommodate requests to restore these files or folders. Each email user is responsible for backing up individual messages and folders as appropriate. In the event of a disaster, the backup would be used to restore the email system to its working state just prior to the disaster. See section 5.3 for more backup details.

Marshall's student email environment (currently Microsoft Live@edu, and a pilot Google Mail) is similarly protected as part of the service contract with Microsoft and Google. Similarly single or multiple file restoration is not possible and Students are urged to be cautious about deleting files and are responsible for providing backup to their individual mailboxes. See section 5.4 for more backup details.

#### 5.6.3 Disposition of Email when the relationship with Marshall is interrupted.

Individuals may leave the University to take other employment jobs, to transfer to another college, or simply to go on to other activities. Since such people

Formatted: Indent: Left: 1"

often have no continuing relationship with the University, their email benefits may be ~~substantially reduced~~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.

#### ~~6.6.3.1~~ Faculty/Staff

##### ~~6.16.3.1.1~~ Faculty/Staff who are dismissed from their employment:

If a faculty or staff member is dismissed from the University 'for ~~Cause-cause~~, access to exchange and live mail to email privileges will be terminated immediately upon a receipt of notification by the Human Resources Department 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~~one-month period. Any requests to be ~~provided~~provided with a copy of email should be directed to the the Chief Human Resources Officer (CHRO) for staff or the University Provost for faculty Provost. Upon request by the ~~Provost~~CHRO or Provost, other members of the University may be granted access to the mailbox ~~in order to~~to conduct the business of the University. Email address forwarding is not available.

Formatted

Formatted

Formatted: Indent: Left: 1.5"

#### ~~6.2~~ Faculty who leave before retirement.

~~6.2.1~~ A faculty member who leaves before retirement may keep his/her business (exchange) email account for 90 days after the end of the last semester in which he/she taught. After this period, the mailbox will be marked for deletion and email will be forwarded to live mail by default. The faculty member is responsible for making any needed backup copies of email during this period. Upon request by the Provost, other members of the University may be granted access to the mailbox in order to conduct the business of the University. Email address forwarding to external mail systems is available.

Formatted

Formatted: Normal, Indent: Left: 1.25", No bullets or numbering

#### ~~6.2.2~~ Faculty who retire from the University.

A faculty member who retires from Marshall University may keep his/her business (exchange) email account for six months after the end of the last semester in which he/she taught. After this period, the mailbox will be marked for deletion and email will be forwarded to live mail by default. The faculty member is responsible for making any needed backup copies of email during

Formatted: Indent: Left: 1.5"

Formatted: Body Text

Formatted: Indent: Left: 1"

this period. Upon request by the Provost, other members of the University may be granted access to the mailbox in order to conduct the business of the University. Email address forwarding to external mail systems is 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.

#### 6.2.36.3.1.3 Faculty/~~or~~ Staff who retire from the University with Emeritus status.

~~For~~ faculty or staff ~~member~~ who retires 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. ~~Outlook account.~~ (See University Emeritus Status of Retired Professionals)

### 7. ~~Staff~~

#### 7.1 ~~A staff member who is dismissed.~~

If a staff member is dismissed from the University 'for Cause', business (exchange) and live mail email privileges will be terminated immediately upon receipt of notification by the Human Resources Department. That person's mailbox will be marked for deletion one month after the

Formatted: Indent: Left: 1.5", No bullets or numbering

Formatted: Body Text

Formatted: Body Text

Formatted: Indent: Left: 1.5"

Formatted

Formatted: Body Text

Formatted: Indent: Left: 1.25"



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 a copy of email should be directed to the Human Resource Office. Upon request by the Director of Human Resources, other members of the University may be granted access to the mailbox in order to conduct the business of the University. Email forwarding to external email systems is not available.

7.2 — Staff who leave before retirement:

A staff member who leaves before retirement may keep his/her business (exchange) email account for 90 days after his/her termination date. After this period, the mailbox will be marked for deletion and email forwarded to live mail by default. The mailbox owner is responsible for making any needed backup copies of email during the period they still have access to the mailbox. Upon request by the Director of Human Resources, other members of the University may be granted access to the mailbox in order to conduct the business of the University. Email address forwarding to external mail systems is available.

7.3 — Staff who retire from the University:

A staff member who retires from Marshall University may keep his/her business (exchange) email account for six months after his/her termination date. After this period, the mailbox will be marked for deletion and email forwarded to live mail by default. The mailbox owner is responsible for making any needed backup copies of email during the period they still have access to the mailbox. Upon request by the Director of Human Resources, other members of the University may be granted access to the mailbox in order to conduct the business of the University. Email address forwarding to external mail systems is available.

8. — Students

6.3.2 Students

8.46.3.2.1 A student who is expelled.

If a student is expelled from the University 'for Cause', email access by the student privileges will be terminated immediately upon receipt of notification by the Dean of Students 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 the Provost or the Vice President of Student Affairs Dean of Students. Upon request by the Dean of Students Provost or Vice President of Student Affairs, University professional staff may be granted access to the

Formatted: Body Text

Formatted: Indent: Left: 1.25"

Formatted: Indent: Left: 0.25"

Formatted: Body Text

Formatted: Indent: Left: 1.25"

Formatted: Not Expanded by / Condensed by

Formatted: Indent: Left: 1", No bullets or numbering

Formatted: Body Text, Don't add space between paragraphs of the same style

Formatted: Indent: Left: 1.5"

mailbox. ~~Email address forwarding to external mail systems is not available.~~ Email address forwarding is not available.

#### 8-26.3.2.2 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 as long as if their leave status has been designated ~~in Banner~~ 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 backup~~needed copies of email during the period that there is still access to the ~~personal~~ mailbox. Upon request by ~~the the~~ Provost or Vice President of Student Affairs Dean of Students, University professional staff may be granted access to ~~a your mailbox~~ student's mailbox. ~~Email address forwarding to external mail systems is available.~~ Email address forwarding is not available.

**Formatted:** Body Text, Don't add space between paragraphs of the same style

**Formatted:** Indent: Left: 1.5"

#### 8-36.3.2.3 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) ~~six~~ months from the last day of the semester where their degree requirements were completed. After these ~~six~~ 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 ~~your the~~ personal mailbox. Upon request by ~~the the~~ Vice President of Student Affairs Dean of Students, University professional staff may be granted access to ~~your a~~ student's mailbox. ~~Email address forwarding is not available.~~ ~~Email address forwarding to external mail systems is available.~~

**Formatted:** Body Text, Don't add space between paragraphs of the same style

**Formatted:** Indent: Left: 1.5"

#### 9-6.4 Email Address Blocking:

~~Blocking unwanted email from particular addresses should be done using client software, unless the offender is attacking and/or hacking computer resources (i.e., spamming, mail bombing, etc.). The University Messaging System administrator may block either the email address or the domain from which that mail is being relayed. If the administrator blocks certain addresses or domains, a notification will be sent to the IT managers distribution list.~~

**Formatted**

**Formatted:** Indent: Left: 1"

~~University Information Technology reserves the right to implement RBLs (Realtime Blackhole List), or a similar product. RBL's are lists of IP addresses of known sources of unsolicited commercial and bulk email (a.k.a. SPAM). The RBL is our first level of defense in our attempt to minimize and manage the impact of spam on our messaging system. 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.~~

**Formatted:** Indent: Left: 1"

#### ~~10-6.5~~ Confidentiality of email:

Authorization for University personnel to monitor or access the electronic communications of individual faculty, staff, ~~and students, and affiliates~~ will not be ~~granted~~ ~~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)~~ ~~usually~~. Such authorization will require justification based on reasonable business needs or ~~reasonably substantiated~~ substantiated allegations of a violation of law or policy on the part of the employee or student. In ~~carrying out~~ conducting the retrieval of files or information, due respect should be accorded to confidential or personal information and legally protected files. Whenever possible, the ~~employee or student should~~ user should be informed and asked to help in obtaining the needed business materials.

**Formatted**

**Formatted:** Indent: Left: 1"

#### ~~11-6.6~~ Group Email Accounts:

Requests for shared departmental accounts will be accommodated, but require a designation of an account holder, who will administer the addition, deletion, or modification of names within the account, ~~as well as manage the account as per these guidelines. 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. These accounts will be created with an expiration date of 1 year, at which time the holder can request a renewal, which will be granted pending verification of identity and the member list. Shorter expiration dates will be given where appropriate, such as to accommodate specific time sensitive needs. Supported types of shared accounts are designated as:~~

**Formatted**

**Formatted:** Indent: Left: 1.55"

**Formatted:** Default Paragraph Font, Font: 12 pt, No underline, Font color: Auto, Pattern: Clear

- ~~Type 1 This id will be able to receive mail from anywhere on the Internet but will have no direct reply capability. The group/organization utilizing this type of generic id will have to utilize their own personal mail id to respond to the originators of any mail received by this generic id. These accounts will only be granted for SGA or Faculty/Staff recognized activities or organizations with approval for the faculty advisor of the organization (for SGA).~~

**Formatted:** Body Text, Indent: Left: 1", Right: 0.19", No bullets or numbering, Widow/Orphan control, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.46" + 0.92"

- ~~Type 2 This id will be able to receive mail from anywhere on the Internet, and will be able to respond directly to the sender. Mail sent from the group account will not reflect the identity of the responder, but will instead carry the identity of the group account. Due to security concerns given the anonymous nature of email originating from these types of ids, no students will be allowed access to Type 2 accounts. If a student is found to have access to these accounts the holder will be notified of the impending removal of the~~

student account. Repeated violations will result in deletion of the type 2 account.

#### 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.

**Formatted:** Font:

**Formatted:** Indent: Left: 0.5", First line: 0.5", Space After: 0 pt

#### 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.

**Formatted:** Space After: 0 pt

**Formatted:** Not Expanded by / Condensed by

**Formatted:**

**Formatted:** No underline

**Formatted:** Normal, Indent: Left: 1", No bullets or numbering

##### 12.1 Verification of Death:

Verification of Death is required prior to any official University actions. Sensitivity to the grieving family is paramount so verification must be gained as tactfully as possible. Verification can be established by: a Death Certificate; a Coroner's Office Report (in the case of victimization); a City or County Recorder's Office; the local U.S. Consulate or ambassadorial office (if outside of the U.S.); or official military correspondence.

##### 12.2 Deceased Students:

In the unfortunate event that a Marshall University (MU) student should pass away, the following procedure will be used by Information Technology (IT):

- The Dean of Students notifies Senior Vice President for Information Technology/CIO of the event. The following information is required so that IT can create an auto-reply message and to ensure that no new email is accepted:
  - MUnet Username or MUID Number of deceased
  - Name of deceased
  - Date of death
- IT will set the account for auto-reply of the deceased. Standard message (subject to change by Dean) is: This is an automated message: This email account is no longer available. You may contact name, title, email, etc., for further information and assistance.
- IT clears the password.
- As of the date of death, the account enters the transition period. At the end of the transition period, the account is terminated.

##### 12.3 Deceased MU Faculty, Staff and Affiliates:

In the unfortunate event that a MU faculty, staff or affiliated person should pass away, the following procedure will be used by IT:

- Vice president of that area notifies IT of the event and IT will change the

account's password and archive the Exchange mailbox in case it's needed later for review.

- ~~MUNet Username or MUID Number of deceased~~
- ~~Name of deceased~~
- ~~Date of death~~
- ~~In the unit to whom external correspondents can be referred, typically the manager, department chair, dean, director, etc. For this individual we need name, title and email address.~~
- ~~In addition, Vice President tells IT who will be responsible for reviewing the email of the deceased to ensure that no official business is outstanding—this person is referred to as the email agent. The email agent would be the person who is entrusted to go through the desk of the deceased to separate personal items from MU business materials.~~
- ~~IT will set the account for auto-reply and do not save messages to the account of the deceased. Standard message (subject to change by the appropriate Vice President) is: This is an automated message: We are sorry to inform you that First name Last name passed away on Month Day, Year. You may contact Responsible First name Responsible Last name, Responsible Title, at Responsible email address.~~
- ~~IT forwards the new password to the person specified in step 2 above (email agent).~~
- ~~Email agent identified by department logs into the deceased's and reviews all existing email to identify any unread messages that require official action/response. These are either replied to or forwarded as appropriate based on context.~~
- ~~Upon completion of the review and handling, the e-mail agent can either delete all messages or ask IT to do so.~~
- ~~IT coordinates termination and/or reassignment of account privileges as described in ITP 40—Marshall IT Procedure for Employee Account Termination. Department should document this request thru the completion of the form ITP 40F Employee Account Termination Form.~~

### 13. OTHER RELATED GUIDELINES

#### ITP 5 Information Systems Identity, Access, Privilege, and Content Retention Procedure

Triggering Event	Wait period	Identity Status	Privilege Status	Ephemeral Content Status	Administrative, Fiscal, or General Content Status	Special Consideration

Death	Immediate	Identities archived not available	Network access suspended, email account suspended, myMU portal access suspended	Content archived for 6 months then deleted	Unchanged, Administration retains ownership	Family given access to ephemeral content if requested
-------	-----------	-----------------------------------	---	--	---	---

#### 14.6.9 Multiple relationships with the University:

~~Some~~ individuals may have more than one affiliation with the University. A faculty member may also be ~~an alumna~~ 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.

Formatted

Formatted: Indent: Left: 1"

#### 15.6.10 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.

Formatted

Formatted: Indent: Left: 1"

~~As a matter of convenience, the University does permit incidental personal use of its email systems provided that such use does not interfere with University operations, does not generate incremental identifiable costs to the University, does not negatively impact the user's job performance, and does not violate the law or any other provision of the Marshall University's Acceptable Use Policy or any other applicable policy/guideline at Marshall.~~

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 Acceptable 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 ~~University~~ the University Police.
- Unauthorized Access - It is a violation of this policy to attempt to gain

Formatted: Indent: Left: 0.93"

access to another person's email files regardless of whether the access was successful or ~~whether or not~~[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 email will also be dealt with and/or reported to the proper authorities.<sup>4</sup>
- 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~~[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 ~~restrictions~~[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~~[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~~[authorities](#).

#### ~~16.6.11~~ 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 ~~generally reliable~~[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.](#)

Formatted

Formatted: Indent: Left: 1"

#### 17-6.12 Email privacy:

While the University respects the privacy of ~~electronic communications~~[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~~[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 ~~handled~~[managed](#) within the following guidelines:

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

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 ~~above~~ to the Chief Information Officer for

Formatted

Formatted: Indent: Left: 1"

Formatted: Indent: Left: 1"

Formatted Table

Formatted: Indent: Left: 1"



processing. If the request is the result of a court order, then written permission from the above authorized person is not required.

~~With the exception of content covered by the University's intellectual property policy, all electronic information residing on University owned systems and all Internet traffic generated through or within these systems, are the property of the University. They are not the private property of any University employee, faculty, staff, contractor, student, or other person.~~

~~18.6.13~~ 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.

**Formatted:** Font color: Auto, Condensed by 0.1 pt

**Formatted**

**Formatted:** Indent: Left: 1"