MARSHALL UNIVERSITY INFORMATION TECHNOLOGY COUNCIL

Procedure ITP-29

ELECTRONIC COMMUNICATIONS PROCEDURE

1. General Information:

1.1. Scope:

This procedure is controlling over the provision and use of electronic communications systems within the Marshall University information technology environment

1.2. Authority: Marshall University Information Technology Council

1.3. Passage Date: April 18, 2014

1.4. Effective Date: April 18, 2014

1.5. Revision Date: August 19, 2019

1.6. Controlling over:

1.6.1. 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 IT – 3. Clarifications were made to this procedure on 4/18/14.

1.8. 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

1.9. 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:

5. Email Procedures:

5.1. Email general information:

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

5.1.1. An internally operated Microsoft Exchange Mail environment for Faculty, Staff, and authorized Affiliates business related Email.

5.1.2. 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.

5.1.3. 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. Email identity and assignment:

5.2.1. 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.

5.2.2. Affiliated Personnel: It is recognized that work requirements for those who are affiliated with Marshall University, though not directly in its employ, may necessitate access to electronic services. Some categories of these affiliates 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:**

5.3.1. 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 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 or, if it is deemed necessary, that their quota be increased. Such requests may be denied. Denials may be appealed. Email backup and retention will be based on a documented risk assessment, and is as follows:

5.3.1.1. Full backups are done weekly. The retention period for these backups is four weeks

5.3.1.2. Incremental backups are done daily. The retention period for these backups is four weeks.

5.3.1.3. 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.

5.3.3. 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

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.

5.3.4. 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 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.

5.4. 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. Disposition of Email when the relationship with Marshall is interrupted:

Individuals may leave the University to take other employment, 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 substantially reduced or terminated. The following situations describe what will happen to the marshall.edu email address.

5.6.1. Faculty

5.6.1.1. Faculty who are dismissed.

If a faculty member is dismissed from the University 'for Cause', 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 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 Provost. 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 is not available

5.6.1.2. Faculty who leave before retirement.

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.

5.6.1.3. 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 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.

5.6.1.4. Faculty or Staff who retire from the University with Emeritus status.

A faculty or staff member who retires from Marshall University with Emeritus status may request continuation of their Outlook account. (See University Emeritus Status of Retired Professionals)

5.6.2. Staff

5.6.2.1. 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 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.

5.6.2.2. 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.

5.6.2.3. 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.

5.6.3. Students

5.6.3.1. A student who is expelled.

If a student is expelled from the University 'for Cause', email privileges will be terminated immediately upon receipt of notification by the Dean of Students. The mailbox will be marked for deletion one month after your 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 Dean of Students. Upon request by the Dean of Students, University professional staff may be granted access to the mailbox. Email address forwarding to external mail systems is not available.

5.6.3.2. Students who leave before graduation.

Students who leave the university without completion of their degree or other program requirements may keep their email account as long as their leave status has been designated in Banner as "current". Once the leave status expires the email account will be marked for deletion. The student is responsible for making any needed backup copies of email during the period that there is still access to the personal mailbox. Upon request by the Dean of Students, University professional staff may be granted access to your mailbox. Email address forwarding to external mail systems is available.

5.6.3.3. Students who graduate or complete program requirements.

Students who complete their degree or other program requirements will maintain their email account for six months from the last day of the semester where their degree requirements were completed. After these six 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 personal mailbox. Upon request by the Dean of Students, University professional staff may be granted access to your mailbox. Email address forwarding to external mail systems is available.

5.7. 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.

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.

5.8. Confidentiality of email:

Authorization for University personnel to monitor or access the electronic communications of individual faculty, staff, and students will not be granted casually. Such authorization will require justification based on reasonable business needs or reasonably substantiated allegations of a violation of law or policy on the part of the employee or student. In carrying out 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 be informed and asked to help in obtaining the needed business materials.

5.9. Group 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. 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:

5.9.1. 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).

5.9.2. 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.

5.10. Protocol for Student, Faculty, Staff and Affiliate Death

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.

5.10.1. 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 e-mail account is no longer available. You may contact name, title, e-mail, 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.

5.10.2. 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
    - Responsible party 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.

5.10.3. 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	Special Consideration

					General Content Status	
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

5.11. Multiple relationships with the University:

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

5.12. 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.

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 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 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 or not 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.

- 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 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.

5.13. 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, timely delivery of time-sensitive information cannot be guaranteed.

5.14. Email privacy:

While the University respects the privacy of electronic 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 handled within the following guidelines:

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

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 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.

5.15. Email policy dispute or interpretation:

Chief Information Officer is charged with the responsibility to periodically review the policy and propose changes as needed.