

MARSHALL UNIVERSITY INFORMATION TECHNOLOGY COUNCIL

Procedure IT- 5

Marshall University Information Systems Identity, Access, Privilege, and Content Retention Procedure

1 General Information:

1.1. Scope: This procedure applies to all individuals or groups, including but not necessarily limited to, faculty, staff, students, contract employees, or other related individuals who have established a relationship with the institution and by doing so acquired an identity and access to any Information System that stores, accesses, or processes information in which the institution holds an interest.

1.2 Authority: Marshall University Information Technology Council

1.3 Passage Date/Last Revision by MUITC: March 10, 2006

Passage Date/Last Revision by MUBOG:

1.4 Effective Date: January 1, 2007

1.5 Controlling over: Marshall University

1.6 History:

1.6.1 Statutory References: West Virginia State Electronic Mail Suggested Guidelines - https://www.state.wv.us/itc/ITC_E-mail_Use_Retention.pdf

1.7 Purpose: This procedure is meant to define the persistence of the following Information Technology entities (please see the definitions section of this procedure):

Identities, e.g., MUNet ID, Email addresses,

Privileges, e.g., levels of access to resources, and systems, and

Content, e.g., electronic files, folders, documents, media, etc..

Persistence of these items needs to be defined and controlled to insure the efficient, cost effective, reliable, and secure operation of information systems and to insure the integrity and security of the information content stored in these systems.

2. Procedure:

2.1 Persistence of Identities: 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. In a similar manner, the MUNet ID and email address will be reserved and not reassigned to another individual. Under this procedure 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 some possibility that a reactivation of this identity will be needed, e.g., returning student, faculty, staff etc., or

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 the same individual.

2.2 Persistence of Privileges: It is the procedure of Marshall University that privileges are assigned based upon an individual’s role within the institution and change as roles change. Such changes in role will be immediately followed or anticipated where possible by a change to the privileges assigned to the individual. At that time the persistence of content policies determine the fate of content associated with the change in privilege assignment.

Privileges are created based upon the role of an individual and, for default privileges, an implicit request, e.g., application, admission, hiring, etc., or for elevated or expanded privileges, explicit administrative approval.

Privileges may be suspended for administrative proposes pending due process procedures and a final determination or by an explicit administrative request.

Privileges will be modified or deleted based upon a role change of an individual and will revert to default privileges from an implicit request, e.g., graduation, non-registration, termination, retirement, resignation, or to lowered or elevated state from an explicit administrative request and approval, e.g., transfer, acquisition of new responsibilities, etc.

2.3 Persistence of Content: It is the procedure of Marshall University to protect and secure all content as documented in the Marshall University Information Security Policy. This persistence procedure specifically deals with the retention of the various categories of content in their availability state over time.

On going:

The retention times are summarized in the following matrix.

	Administrative	Fiscal	General	Ephemeral
Online	Determined by Marshall University Document Retention Policies and Practice			90 days
Near-online	Determined by Marshall University Document Retention Policies and Practice			User/Owner Responsibility
Archived	Determined by Marshall University Document Retention Policies and Practice			User/ Owner Responsibility
Pending Deletion	weekly	weekly	weekly	weekly

As a result of changes to identity or privilege:

Triggering event	Wait period	Identity status	Privilege status	Ephemeral Content status	Administrative, Fiscal, or General Content status	Special Consideration
Identity Change	immediate	Old ID archived not available	New ID default plus approved extensions.	Moved by user within 30 days, old content archived for 6 months then deleted	Unchanged, Administration retains ownership	
Identity Abandonment or unused accounts:	If account not used for 1 year	Identities Archived available	Network access suspended, email account suspended, myMU portal access suspended	Content archived for 6 months then deleted	Unchanged, Administration retains ownership	
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
Computer abuse investigation:	immediate	No change	Network access suspended, myMU portal access suspended	Content remains unchanged but inaccessible	Unchanged, Administration retains ownership	
Computer abuse sanction:	immediate	Determined by sanction	Determined by sanction	Determined by sanction	Unchanged, Administration retains ownership	Determined by sanction
Employee (faculty or staff) termination	immediate	No change	Revert to default	No change	Unchanged, Administration retains ownership	Role reverts to affiliate by default. Administration may change disposition based on nature of termination.
Transient access (contract, part-time, student employees) no longer needed:	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	
Student	immediate	No change	Revert to	No change	Unchanged,	Role changes to

“resignation” (graduation, non-registration, withdrawal, suspension):			default		Administration retains ownership	Formal or informal alumnus
Employee (faculty or staff) resignation	immediate	No change	Revert to default	No change	Unchanged, Administration retains ownership	Role reverts to affiliate
Employee (faculty or staff) retirement:	immediate	No change	Revert to default	No change	Unchanged, Administration retains ownership	Role reverts to “emeritus”
Employee (faculty or staff) transfer:	immediate	No change	Revert to default. Add approved extensions	No change	Unchanged, Administration retains ownership	Role changes with new assignment
Employee (faculty or staff) leaves, disabilities or sabbaticals	immediate	No change	No change	No change	Unchanged, Administration retains ownership	Changes to identity, privilege, or content is determined case by case, default is no change

3. Enforcement: It is the responsibility of the Vice President for Information Technology and CIO to enforce this procedure. The routine enforcement of this procedure has been assigned to the Assistant Vice President for Information Technology by the Vice President.

4. Definitions:

4.1 Identities: For the purposes of this procedure, identities include the MU ID, MUNet ID and email address assigned to an individual who has established a relationship with Marshall University.

4.2 Privileges: For the purposes of this procedure, privileges include the ability to authenticate and gain access to an information system, network, or storage device and media, to access (create, read, write, modify, or delete) information on an information system, network, or storage device and media, or to manipulate (establish, modify, suspend, revoke) the privileges of yourself or others.

4.3 Roles: For the purposes of this procedure, roles are generally defined by the following:

Affiliate (e.g., WVNET/MU Dialup Service External Account Holder, Contractor
external collaborator, external evaluator, external auditor, etc.)

Prospective Student

Admitted Student

Enrolled Student

Formal Alumni

Informal Alumni

Full time Faculty

Part time Faculty

Faculty Emeritus

Full time Employee

Part time Employee

Retired Employee

Temporary Employee

Student Employee

4.4 Default Privileges: The default privileges afforded an assigned MUnet identity (account) are:

logon privilege to MUnet as a domain user,

a V-Drive allocation and access,

an Email account, space allocation, and access, and

myMU portal access

4.5 Content: For the purposes of this procedure, content includes electronic files, folders, documents, media, etc. that are created by use of information systems. These include but are not limited to, voice mail, email, electronic documents, scanned images, music, videos,

pictures, art, drawings, plans, program source, object, and executables, scripts, parameter and configuration files, data bases, etc. These content items are further categorized as administrative, fiscal, general, or ephemeral.

Administrative content is defined as any content that is related to the specific administration and operation of the institution that is essential for the continued operation of the institution and to the documentation, audit trail, and history of the institution for both legal and administrative purposes.

Fiscal content is defined as a subset of administrative content that documents or manipulates fiscal related information, policies, procedures, or records.

General content is defined as other miscellaneous content that although not essential further documents the operation and history of the institution.

Ephemeral content is anything not assigned to the three other categories but is principally content that could be considered personal or professional that is perhaps considered important by an individual or group but not necessarily related to the administration of Marshall University.

Content can also be categorized by its location or availability state. Content can be found online, near online, archived, or pending deletion and generally moves in that order over time and possibly results in deletion or destruction.

Online content is content stored in information systems available for immediate access.

Near-online content is content stored in hierarchical storage systems for delayed access.

Archived content is content stored on archival media (or backup form) for occasional access for historical or backup restoration purposes.

Content **pending deletion** is content stored in a state or location, sometimes referred to as a wastebasket immediately preceding its deletion or destruction.