Marshall University Information Technology Council

Procedure ITP- 5

Marshall University IT 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:

March 10, 2006

1.4. Effective Date:

January 1, 2007

1.5. Revision Date:

August 19, 2019

1.6. Controlling over:

Marshall University

1.7. History:

1.8. Statutory References:

West Virginia Email Use Standards Policy

1.9. 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 ensure 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 access is 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 determines 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 IT-2 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.

2.3.1. Ongoing:

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:

2.3.2.

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 18 months	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

Triggering event	Wait period	Identity status	Privilege status	Ephemeral Content status	Administrative, Fiscal, or General Content status	Special Consideration
Employee (faculty or staff) termination	immediate upon request	No change unless requested by the department	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 upon request	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 "resignation" (graduation, non-registration, withdrawal, suspension):	Immediate upon request	No change	Revert to default	No change	Unchanged, Administration retains ownership	Role changes to Formal or informal alumnus
Employee (faculty or staff) resignation	Immediate upon request	No change	Revert to default	No change	Unchanged, Administration retains ownership	Role reverts to affiliate
Employee (faculty or staff) retirement:	Immediate upon request	No change	Revert to default	No change	Unchanged, Administration retains ownership	Role reverts to "emeritus"
Employee (faculty or staff) transfer:	Immediate upon request	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 upon request	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. Routine Network Account Cleanup

On a regular scheduled basis, the IT Infrastructure Systems team evaluates account activity throughout our AD domain and perform account cleanups. Our process is as follows:

ITI Systems team identifies a subset of the population to "disable". Generally, it is a query of all users in the Users and Office365 OUs in AD based.

3.1.

From that list of users, we query every domain controller to get the user's most recent *lastLogonTimestamp* attribute. If the attribute is greater than 18 months, we add them to the list to be processed.

3.2.

Once the list is generated, we add those email addresses to a list on university mailing lists lists.marshall.edu which is then notified at least once a month for 3 months.

3.3.

After the three-month notification window, we rerun the script to capture everyone that has not logged in for 21 months (the initial 18-month window + the three-month notification window). This list, once generated, is run through a final process.

3.4.

The final process involves, capturing the user's email address, UPN, *lastLogonTimestamp*, and their DN. We then do the following for every account:

3.5.

Disable the account

3.6.

Move the account to the Disabled Users OU

3.7.

Append to their notes field stating the account was disabled due to inactivity followed by the date/time of disabling and move, the user performing the change, and the CR/TIC/SR number to reference.

4. Banner Account Deprovisioning

The process of reviewing a user's Banner Access will usually begin by receiving a request from their current Supervisor wanting to assign new Banner Access for the employee. When the employee's Banner Access is reviewed and evaluated, a notice with the employee's current access level is sent to the employee's supervisor to review and send updates to Enterprise Applications to make changes.

The process to terminate a user's Banner access begins by either receiving an email or a Banner Termination Form from the supervisor of terminated employee in question. Once a termination request is received, the Banner users account is disabled by applying the USR_DEF default role to the account. This role does not allow the terminated employee to create a banner session.

For periodic access review, a Banner access report is sent to each supervisor every 6 months for review of each employee's current access rights into Banner. If there are any changes to be made to the employee's access level, IT Enterprise Applications team is notified of the changes and are applied to the Banner users account.

5. Enforcement:

It is the responsibility of the Chief Information Officer to enforce this procedure.

6. Definitions:

6.1. Refer to ITP-10 for Terms and Definitions.