MARSHALL UNIVERSITY INFORMATION TECHNOLOGY COUNCIL

Procedure ITP-45

ELECTRONIC RECORDS MANAGEMENT PROCEDURE

1 General Information

1.1 **Scope:** This procedure applies to all Marshall University electronic records created or acquired in the course of university business.

1.2 **Authority:** Marshall University Information Technology Council

1.3 **Passage Date**:

1.4 Effective date:

1.5 **Controlling over:** Marshall University

1.6 **History:** This procedure follows Marshall University policy IT-6 Electronics Records Management Policy on electronic records management.

1.7 **Background:** The electronic records management procedure of Marshall University seeks to:

1.7.1 Provide guidance to staff and faculty of Marshall University concerning the proper use, storage, and disposal of electronic records with respect to records management best practices, and state and national laws and regulations.

1.7.2 Inform staff and faculty on how to best preserve electronic records for the long term, in order to preserve essential parts of Marshall's history.

2 Definitions

2.1 **Records Custodian.** Each academic or administrative unit will designate a records custodian who is responsible for the day to day transactions related to the administrative unit's records (both electronic and paper) related functions and manages the disposition of records at the conclusion of the designated retention period.

2.2 **Data Classification.** Data classification is a major part of electronic records management. Data classification will determine what the records are, who they belong to, and will help determine where they end up later. Important parts of data classification are:

2.2.1 Determining if a record belongs to Marshall University, or an outsider.

2.2.2 Determining if an item is a draft or final copy. Drafts are not records and do not need to be kept.

2.2.3 Determining if a record is a convenience copy or master record copy. Master record copies—the official final version of a document—only need to be stored or archived by the department identified as owner or steward. Convenience copies by other departments only need to be kept as long as needed for business purposes.

2.2.4 Determining which department is the owner or steward of the master record copy. This process will reduce the confusion regarding each department's responsibilities and establish an inventory of the ownership and location of master record copies.

3 Roles and responsibilities:

3.1 The University Archivist and Records Management Librarian (ARML) will do the following:

3.1.1 Conduct and oversee the inventory and appraisal of all University records as required.

3.1.2 Conduct and oversee the preparation and maintenance of the department records retention schedule program.

3.1.3 Encourage adherence to the agency records retention schedules.

3.1.4 In conjunction with the Information Technology Division, establish the metadata schema for electronic records.

3.1.5 Approve all documentation for transfer of records to the University Archives.

3.1.6 Approve requests to dispose of University records as designated by an approved records retention schedule.

3.2 The University Information Technology Department will:

3.2.1 Specify all technical characteristics necessary to read and process the electronic records.

3.2.2 Identify all defined inputs and outputs of the system.

3.2.3 Suggest naming conventions and the contents of the files and records created electronically.

3.2.4 In conjunction with the Archivist and Records Management Librarian, establish the metadata schema for records created electronically.

3.2.5 Determine restrictions on access and use in conjunction with the archivist and records management librarian.

3.2.6 Describe update cycles or conditions and rules for adding, modifying, or deleting records.

3.2.7 Encourage the timely, authorized disposition of electronic records as indicated by the records retention schedule.

3.2.8 Maintain the integrity of the electronic records created by the University.

3.2.9 Plan and implement the backup of electronic records to include a disaster recovery plan for the electronic records management program.

3.3 The Department/College has the following requirements:

3.3.1 Publish the unit's record management policies electronically so that it is accessible to university personnel.

3.3.2 Implement the unit's record management practices and conduct periodic in-service~~s~~ training for unit personnel and information sessions for new employees.

3.3.3 Ensure that the unit's management practices are consistent with the electronic records management policy.

3.3.4 Ensure that access to confidential records and information is restricted.

3.3.5 Destroy inactive records upon passage of the applicable retention period and record that this has been done, unless there is a litigation hold, or chance for one that affects said records.

3.3.6 Conduct a records inventory with the ARML

3.3.7 Designate a records custodian in writing who is responsible for following the records retention requirements applicable to that particular unit. Records management should be a part of the records custodian's Position Information Request (PIQ), if applicable.

3.3.8 Collaborate with the IT Division personnel to migrate electronic files to new formats if necessary during the time they are in the department.

3.3.9 Conference with the University Archives regarding the transfer of master records to permanent archival storage.

4 Procedure:

4.1 Records Survey. An electronic records survey will be conducted by the unit and overseen by the unit custodian, with assistance and training from the records manager and relevant IT personnel.

4.1.1 The survey will identify all electronic records created and/or used by the unit in the conduct of normal university business.

4.1.2 The survey will identify the purpose of the record, the master record copy holder, the electronic properties of the file, the current location of the record and any statutory or legal requirements associated with the record.

4.1.3 Each administrative office or unit will ensure that their electronic records are reflected in their overall records retention schedule (See appendix 1 for sample schedule).

4.2 Records and Establishing Metadata and File Naming Conventions. The unit records custodian, the university archivist and records management librarian (ARML), and appropriate IT personnel will work together to create a metadata schema and file naming conventions that best fit the unit's needs, based on information garnered in the electronic records survey.

4.2.1 Standardized Formats. Many file formats are proprietary and are not appropriate for long term storage. For the best results, files should be saved in the following formats:

- Text Files: PDF or PDF/A, Extensible Markup Language (XML)
- Images: Uncompressed TIFF, JPEG2000 (lossless), PNG
- Audio: Broadcast Wave file, Free Lossless Audio Codec (FLAC)
- Video: Uncompressed AVI, Digital Moving Picture Exchange Bitmap (DPX)
- Spreadsheet: Comma separated values (CSV)
- Presentations: OpenDocument Presentation Format (ODP), PDF, PDF/A

4.2.2 Minimum metadata requirements. Minimum metadata requirements are based on Dublin Core's Metadata Element Set, which includes:

- Title: Formal or working title of the document
- Creator: Original author of the record
- Subject: Overarching topic the record covers
- Description: A short note describing the record
- Source: Which office or department the document originated from
- Date (s): When the document was created, published, and submitted.
- Type: What kind of record this is, i.e. a memo, e-mail, meeting minutes, etc.
- Format: File format, i.e. PDF, Microsoft Word document, etc.
- Relation: Documentation of the interrelation of different records
- Rights: Copyright data if applicable.
- Additional metadata elements may be required as needed.

4.2.3 File naming conventions. Title should include a detailed and accurate description of what the file is. While each department will need to determine their own file naming conventions, the following is a basic list of suggested requirements in titles.

- Version number
- Date of creation
- Name of creator
- Description of content
- Name of intended audience
- Name of group associated with the record
- Release date
- Publication date
- Project number
- Version type, i.e. "draft"

4.3 Access and Security

4.3.1 Confidentiality. Many records subject to record retention requirements contain confidential information. In addition to the retention requirements, any record that contains confidential information should be considered confidential and stored and secured accordingly. These records should only be accessed by appropriate university staff when necessary.

4.3.2 Circumstances where it is appropriate for university staff to access private records include:

- When the university must monitor records systems to avoid hazards to the records systems; i.e., to scan for viruses.
- When the university has a genuine business need to access records.
- When there is reasonable cause to believe that misconduct has occurred.

4.3.3 Confidentiality is protected by:

- The Health Insurance Portability and Accountability Act (HIPAA), which protects personal health information.
- The Family Educational Rights and Privacy Act (FERPA), which protects personal and educational information.
- The Gramm-Leach-Bliley Act (GLB), which protects personal financial information.
- Other legislative acts or contractual agreements.

4.3.4 Confidentiality cannot be guaranteed in cases of:

4.3.4.1 Information falling under the West Virginia Freedom of Information Act (FOIA). This act dictates that all U.S. citizens are entitled to information about the affairs of public officials and organizations. This does not apply to information protected by HIPAA, FERPA or GLB.

4.3.4.2 Information required for a litigation hold or compelled under subpoena by a court of competent jurisdiction or government agency.

4.3.5 Storage of confidential information. Confidential information must be stored securely at all times. Electronic records must be kept on secured servers that are adequately protected with contemporary anti-virus software. Employees also have an obligation to avoid activities that might compromise electronic information, such as browsing websites prone to viruses and downloading from unknown sources.

4.3.6 Compliance with Freedom of Information Act Requests (FOIA). Marshall University is a public university, and hence is required to provide information to the public in compliance with the West Virginia Freedom of Information Act. This information does not extend to the private information of students or staff, which is protected by HIPAA, FERPA, and GLB.

4.3.7 Virus protection. All users have a responsibility to take reasonable actions to prevent virus corruption. This means updating and using University recommended virus protection and browsing or downloading from insecure or questionable websites.

4.4 E-mail: Disposition of e-mail is covered by ITP-29.

5 Storage:

5.1 Department Storage: Departments may establish their own storage for various records of active and inactive use. This storage should exist within shared servers, SharePoint, or similar systems. Personal computers, flash drives, and other media that is not backed up are not suitable record storage.

5.2 Permanent Archival Storage: Permanent Archival records will be transferred to the archives when they reach the end of their useful life in the unit. A separate procedure will explain this process.

5.3 University Learning Management System: While this is an appropriate storage place for content during the duration of a class, faculty should note that course content and student activity data housed on the university's learning management system are stored for a rolling period of 24 months. Instructors must archive course content files and student data reports if they wish to retain these materials for use beyond this period

6 Sources:

"Appendix A: Tables of File Formats." *National Archives and Records Administration*. National Archives and Records Administration. Web. 17 Nov. 2015. http://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html

"BU Libraries Digital Preservation Policy » Digital Initiatives & Open Access | Boston University." *Digital Initiatives Open Access RSS*. Web. 17 Nov. 2015. http://www.bu.edu/dioa/openbu/boston-university-libraries-digital-preservation-policy/.

"Disposal of Records (44 U.S.C. Chapter 33." *National Archives and Records Administration*. National Archives and Records Administration. Web. 17 Nov. 2015. http://www.archives.gov/about/laws/disposal-of-records.html.

"Electronic Records Management Guidelines." *Electronic Records Management Guidelines, File Naming*. Web. 17 Nov. 2015. http://www.mnhs.org/preserve/records/electronicrecords/erfnaming.php.

"West Virginia Code." *West Virginia Code*. Web. 17 Nov. 2015. http://www.legis.state.wv.us/wvcode/code.cfm?chap=29b.