UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-3

RECORD RETENTION POLICY

1 General Information.

1.1 Scope: This policy requires that different types of business records of Marshall University be retained for specific periods of time as listed in a separate records retention schedule, and that outdated records are properly destroyed.

1.2 Authority: W.Va. Code §18B-1-6 and §5A-8-1

1.3 Passage Date: October 30, 2012

1.4 Effective Date: Upon passage

1.5 Controlling Over: Marshall University

1.6 History:

1.6.1 This policy is replacement of the interim retention policy approved by the Board on October 16, 2007.

1.6.2 Additional policy references: Marshall University Board of Governors Policy IT-2, Information Security Policy.

2 Statement of General Policy.

2.1 Marshall University requires that university records, as defined herein, regardless of format, be disposed of or retained for specific periods of time in accordance with legal or other institutional requirements, or for historical value. The university has designated official repositories to manage the retention and disposal of these records according to procedures outlined in this document. Federal and state laws, regulations and best practices require that the University adhere to certain record retention requirements and periods of retention. The appropriate time periods for record retention are record-specific and are subject to ongoing modification from time to time by government statute or regulation, judicial or administrative consent order, private or governmental contract, pending litigation or audit requirements. Such modifications supersede the retention period for the applicable record stated in the Retention Schedule Procedure. Marshall University requires that records be maintained in a consistent and logical manner and be retained in such a manner so that Marshall University can:

2.1.1 Meet legal standards for protection, storage, and retrieval;

2.1.2 Protect the privacy of students, patients, and employees of the University;

2.1.3 Make the most efficient use of limited space;

2.1.4 Minimize the cost of record retention;

2.1.5 Destroy outdated records in a proper manner; and

2.1.6 Retain records that are valuable to the preservation of the University's history.

2.2 Retention periods adopted in this policy may increase by government regulation, judicial or administrative consent order, private or governmental contract, pending litigation, or audit requirements. Such notifications or events may change the retention periods listed in this policy.

2.3 Any record that is the subject of litigation or pertaining to a claim, audit, agency investigation, or enforcement action should be kept until final resolution of the action. Record destruction will be delayed by any of the above reasons and shall be communicated by the Office of General Counsel to various administrative units.

2.4 If the University reasonably anticipates litigation or government agency investigation, the Office of General Counsel shall notify the various administrative units to preserve potential relevant documents until final resolution of the matter.

3 Definitions.

3.1 Administrative Unit: the department, office, college, division, etc., acting as an entity within the institution with a chair or official-in-charge and possibly having other administrative units reporting to said unit. This term is sometimes used synonymously with the generic term "department."

3.2 Business Record: a financial or operational record that is currently being used, or will be used, by the administrative unit that received or generated the record. Records may remain active for varying numbers of years, depending on the purposes for which they were created. The unit has the responsibility of determining the access required and the security needed for the records. Business records can be electronic records.

3.3 Confidential Records: records that contain confidential student, patient, or employee information. Such records should have access limited to "need-to-know" individuals and should be protected from inadvertent access or disclosure.

3.4 Confidential Information: any information that is received or created that includes protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA), personal and educational information under the Family Educational Rights and Privacy Act (FERPA), or any personal financial information under the Gramm-Leach-Bliley Act (GLB). This includes, but is not limited to, name, address, social security number, bank account numbers, financial or financial aid information, student numbers, and medical information.

3.5 E-Mail (electronic mail, Email Instant Messaging etc.): any communication that requires an electronic device for storage and/or transmission. E-mail often refers to a package of services designed to automate office communications.

3.6 Electronic Records: records created or stored by electronic means, including, but not limited to, digital files, images, objects, files on tape, disks, or internal memory.

3.7 Electronic Record Management System (also known as Record-keeping Systems): any electronic system that manages the storage, location, and retrieval of records, either paper or electronic.

3.8 Litigation Hold: a communication issued as the result of current or anticipated litigation, audit, government investigation or other similar matter that suspends the normal process regarding the retention and disposition of University records.

3.9 Metadata: structured data about data. It is information about a record and which describes a record. It is descriptive information about an object or resource whether it is physical or electronic. For example, in an e-mail, the "to:", "from:", "date:", "subject:" etc., would be the metadata. In a word processing document the summary portion of properties would be the metadata. When electronic records are collected or transferred to other media, the appropriate metadata needs to follow the electronic records. Metadata can be manually created or derived automatically using software.

3.10 Record: any information, regardless of physical form or characteristics, made or received in connection with the transaction of University business in accordance with law or regulation. A record may include a document, correspondence, recordings, reports, studies, data maps, drawings, photographs or e-mail, whether in paper, electronic or other form.

3.11 Responsible Department: the department or other administrative unit designated as having the responsibility for retention and timely destruction of the particular types of University records in their control.

3.12 Record Retention and Disposition Schedule: an internal schedule that sets forth how records should be handled after the period of their active use.

4 Electronic Records.

4.1 Information maintained in electronic format does not have a different status just because it is electronic. Issues concerning the Freedom of Information Act, privacy protection, legal discovery, retention, and disposition apply to information in electronic format.

4.2 If official business is conducted via e-mail, even if over privately-owned equipment, it is subject to the same rules and regulations as hard copy records.

5 Unit Responsibilities.

5.1 Vice presidents and/or their designee(s) are responsible for creating administrative procedures for establishing appropriate record retention management practices in their administrative units. Each vice president or designee must:

5.1.1 Publish electronically, the unit's record management policies so that it is accessible to unit personnel;

5.1.2 Implement the unit's record management practices and conduct periodic in-services for unit personnel and information sessions for new employees;

5.1.3 Ensure that these management practices are consistent with this policy;

5.1.4 Educate staff within the unit in understanding sound record management practices;

5.1.5 Ensure that access to confidential records and information is restricted;

5.1.6 Destroy inactive records upon passage of the applicable retention period; and

5.1.7 Ensure that records are destroyed in a manner that is appropriate for the type of records and information involved.

5.2 Vice presidents shall have latitude with respect to which types of records shall have specific retention periods, except that respective vice presidents shall include retention periods for the following types in their administrative procedures:

5.2.1 Financial Records

5.2.2 Human Resources Records

5.2.3 Administrative Records (procurement, real property and other assets, etc.)

5.2.4 Research-related Records

5.2.5 Student Affairs Records

5.2.6 Financial Aid Records

5.2.7 Information Technology including Archives

5.3 If records are not listed, it does not mean that they can or should be destroyed without first considering the general requirements in this policy.

6 Confidentiality Requirement.

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.

7 Disposal and Destruction of Records.

7.1 If a determination has been made, pursuant to this policy, authorizing the disposal of certain records, they must be destroyed in one of the following ways:

7.1.1 Recycle or shred non-confidential paper records;

7.1.2 Shred or otherwise render unreadable confidential paper records; or

7.1.3 Permanently erase or destroy electronically stored data in a manner that renders it unrecoverable. Such a manner shall be determined by the University's chief information officer.

7.2 Periodic reviews are required of records generated and maintained electronically in the University's information systems or equipment (including all computer and data storage systems) to ensure that these requirements are met.

8 General Retention Requirements for Records.

The retention period will be set forth in the University's Record Retention Schedule.

9 Review Date.

The policy and retention schedule will be reviewed annually based on best practices.