UNIVERSITY POLICY FOR GENERAL ADMINISTRATION

Policy No. UPGA-10

INFORMATION SECURITY POLICY

1.1. General Information:

- Statutory References: WV. Code § 18 B-1-6
- Passage Date: September 12, 2019
- Effective Date: October 15, 2019

1.2. Scope:

This Policy applies to all faculty, staff and third-party Agents of the University as well as any other University affiliates who are authorized to access Institutional Data.

1.3. Background:

Marshall University (University") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, integrity and availability of institutional Data as well as any Information Systems that store, process or transmit Institutional Data

2. Definitions:

2.1. "Agent" For the purpose of this Policy, is defined as any third-party that has been contracted by the University to provide a set of services and who stores, processes or transmits Institutional Data as part of those services.

2.2. University Information Technology Council ("ITC") The official university committee advising university wide policy for Information Technology Resources usage at Marshall University. The council will create subcommittees as needed, with membership beyond itself to facilitate its work.

2.3. "Information System" is defined as any electronic system that stores, processes, or transmits information.

2.4. "Institutional Data" is defined as any data that is owned or licensed by the University

3. Policy:

3.1. Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved by the CIO and maintained by the Information Security Officer, given the level of sensitivity, value and criticality that the Institutional Data has to the University.

3.2. Any Technology Resources that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate according to the ITG-4 Guideline for Data Classification.

3.3. Individuals who are authorized to access Institutional Data shall adhere to the administrative procedure ITP-27 Information Security Roles and Responsibilities, as defined in documentation approved by the CIO and maintained by the Information Security Officer.

3.4. Maintenance:

This Policy will be reviewed by the University's Information Security Office on an annual basis or as deemed appropriate based on changes in technology or regulatory requirements.

3.5. Enforcement:

Violations of this Policy may result in suspension or loss of the violator's use of or privileges to Institutional Data and University owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal, and equitable remedies may apply.

3.6. Exceptions:

Exceptions to this Policy must be approved by the Information Security Office, under the guidance of the Chief Information Officer and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

4. Related Policies, Administrative procedures and Guidelines

4.1. Information Security Roles and Responsibilities
http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itp-27.pdf

4.2. Guidelines for Data Classification
http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itg-4.pdf

4.3. Marshall University IT Information Security Incident Response Procedure
http://www.marshall.edu/itc/itcpolicies&procedures/pdf/itp-19.pdf