MARSHALL UNIVERSITY BOARD OF GOVERNORS

Policy No. IT-1

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

1 General Information:

1.1 **Scope:** This Information Technology Resources Acceptable Use Policy (AUP) sets forth the general rights and responsibilities common to all uses of information technology. It applies to any user of the University's information technology resources, whether initiated from a computer located on or off-campus. This includes any computer and information system or resource, including means of access, networks, and the data residing thereon. This policy applies to the use of all University information technology resources whether centrally administered or locally administered. This policy applies to all members of the University community, including guests who have been given accounts on the University's information technology systems for specific purposes. Administrators of individual or dedicated University resources may enact additional policies specific to those resources provided they do not conflict with the provisions of this and other official policies and laws. Users are subject to both the provisions of this policy and any policies specific to the individual systems they use.

1.2 **Authority**: W. Va. Code §18B-1-6

1.3 **Passage Date:**

1.4 **Effective Date:** Upon passage

1.5 **Controlling over:** Marshall University and all units that are directly associated with the institution.

1.6 **History:**

1.6.1 **Statutory References:** W. Va. Code §61-3C-3

1.6.2 MUBOG IT-1 policy replaces the original Computer Use and Abuse Policy and is authorized by the Information Technology Council effective April 8, 2005. This is an update to the version passed by the Marshall University Board of Governors on March 8, 2006.

2 Policy:

2.1 **Introduction**

Marshall University is an academic community dedicated to creating and maintaining an environment for learning that promotes respect for and appreciation of scholarship, freedom, and human diversity. In keeping with this commitment, Marshall University makes certain University computing resources are available to faculty, staff, and students. These resources include educational, research, and communication facilities, disk storage, and selected software. Access to and usage of these facilities is a public

trust; and certain expectations, responsibilities and requirements are inherent to this trust. Access to these finite resources is a privilege and is provided with an expectation of responsible and acceptable use. In addition to the principles and guidelines provided in this policy, institutional policies along with certain federal, state and local regulations apply to the use of the Information Technology Environment (ITE).

2.2 General Principles and Guidelines

The basic premise of this policy is that responsible and acceptable use of the Marshall University ITE does not extend to whatever an individual is capable of doing. Instead, certain principles provide a guide to users regarding responsible and acceptable behaviors and users are responsible for knowing and understanding them. These principles and guidelines include, but are not limited to:

2.2.1 The Marshall University ITE was funded and developed for the sole purpose of promoting and supporting the mission of the University.

2.2.2 Authorized users of the Marshall University ITE, or University sponsored remote resources, are those individuals who have been granted a username and password. The username and password combination is your identity and license to access and use the components of the Marshall University ITE for which you are specifically authorized.

2.2.3 Authorized users will abide by institutional policies along with applicable local, state and federal regulations.

2.2.4 The resources of the Marshall University ITE are finite and shared. Appropriate and responsible use of these resources must be consistent with the common good. The ITE may NOT be used for commercial or profit-making purposes.

2.2.5 The University reserves the right to limit access to the Marshall University ITE when investigating cases of suspected abuse or when violations have occurred.

2.2.6 The University does not monitor or generally restrict the content of material stored on or transferred through the components of the ITE. Use of the ITE is a privilege and not a public forum, therefore the University reserves the right to restrict or deny usage of the ITE when such usage does not promote or support the mission of the University.

2.2.7 Users must adhere to the ethical standards governing copyright, software licensing, and intellectual property.

2.2.8 Personal web pages may NOT contain the official Marshall University logo.

2.2.9 "Mass Mailings" are defined as excessive, unauthorized, and frivolous mailings of two hundred or more identical or nearly identical pieces of electronic communication sent by user or users to other email or voice recipients and are not allowed without approval. The details for approval are found in IT-3.

2.2.10 Unauthorized scanning of ports, computers and networks is prohibited.

2.2.11 Unauthorized attempts to circumvent data protection schemes or uncover security vulnerabilities are prohibited.

2.2.12 Connecting unauthorized equipment to the campus network or computers is prohibited.

University authorized business and other activities directly related to the academic mission of the University are excluded; however, network communication devices must have prior approval from the Division of Information Technology before they can be connected to the campus network. Unauthorized network communication devices or any networked device that may negatively impact management, reliability or integrity of the campus network or other University resource may be disconnected from the network.

2.2.13 Attempting to alter any University computing or network components without authorization or beyond one's level of authorization, including but not limited to bridges, routers, hubs, wiring, and connections is prohibited.

2.2.14 Utilizing network or system identification numbers or names that are not assigned for one's specific use on the designated system is prohibited.

2.2.15 Using campus resources to gain unauthorized access to any computer system and/or using someone else's computer without their permission is prohibited.

2.2.16 Providing services or accounts on University computers or via University networks to other users from a personal computer, unless required to meet the normal activities of students working as individuals or in collaborative groups to fulfill current course requirements, is prohibited. Conducting University-authorized business and other activities directly related to the academic mission of the University is allowed; however, any computers running services that may negatively impact management, reliability or integrity of the campus network or other University resource may be disconnected from the network.

2.2.17 Registering a Marshall University IP address with any other domain name is prohibited.

2.2.18 Commercial use of the University's information technology resources is strictly prohibited for unauthorized commercial activities; personal gain; and private, or otherwise unrelated to the University, business or fundraising. This includes soliciting, promoting, selling, marketing or advertising products or services, or reselling University resources.

2.3 **Enforcement**

Violation of these guidelines constitutes unacceptable use of information resources, and may violate other University policies and/or state and federal law. Suspected or known violations should be reported to the Office of the Senior Vice President for Information

Technology/CIO. The appropriate University authorities and/or law enforcement agencies will process violations. Violations may result in revocation of computing resource privileges, academic dishonesty or Honor Council proceedings, faculty, staff or student disciplinary action, or legal action.

The maintenance, operation, and security of computing resources require responsible University personnel to monitor and access the system. To the extent possible in the electronic environment and in a public setting, a user's privacy will be preserved. Nevertheless, that privacy is subject to the West Virginia Access to Public Records Act, other applicable state and federal laws, and the needs of the University to meet its administrative, business, and legal obligations.

2.4 **Common Forms of Violations**

Although most users strive for acceptable and responsible use of the ITE, inexperienced users may unwittingly engage in behaviors that violate the principles and guidelines of responsible and acceptable use. To that end, this section outlines some of the more common forms of violations that occur. These examples should not be interpreted as an exhaustive list of violations.

2.4.1 Furnishing false or misleading information or identification in order to access another user's account

2.4.2 Using another person's username/password or letting someone else use your username/password

2.4.3 Investigating, reading or attempting to access another user's files without permission

2.4.4 Attempts to access or manipulate certain components of the information technology environment without authorization

2.4.5 Alteration of software, data, or other files without authorization

2.4.6 Disruption or destruction of equipment or resources

2.4.7 Using subterfuge to avoid being charged for computer resources or deliberate, unauthorized use of another user's account to avoid being billed for services

2.4.8 Copying or attempting to copy data or software without authorization

2.4.9 Sending mail or a program which will replicate itself or do damage to another user's account

2.4.10 Interfering with legitimate work of another user

2.4.11 Sending abusive, harassing, or obscene messages

2.4.12 Viewing or listening to objectionable, obscene, pornographic, or harassing material in public areas

2.4.13 Excessive recreational use of resources

2.4.14 Sending chain letters or unauthorized mass mailings or transmitting a crippling number of files across a network

2.4.15 Sending hoax messages or forged messages, including messages sent under someone else's username

2.4.16 Any activity or action that violates the University's Student Code of Conduct or Policies, faculty/staff policies and regulations, or federal, state, or local laws