

# MARSHALL UNIVERSITY BOARD OF GOVERNORS

## Policy No. IT-1

### INFORMATION TECHNOLOGY TERMS OF USE POLICY

#### 1 General Information:

- Authority: Marshall University Board of Governors, WV. Code §18B-1-6 - Rulemaking
- Passage Date: September 12, 2019
- Effective Date: October 15, 2019
- Controlling over: Marshall University and all units that are directly or indirectly associated with the institution.

#### 1.1. Purpose:

This policy explains and stipulates the practices and constraints that a user must agree to for access to the Marshall University Information Technology Resources including all internal and external technology resources.

#### 1.2. Scope:

This Information Technology Resources Terms of Use Policy (TUP) applies to any user of the Marshall University Information Technology Resources, whether initiated from a computer or device 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. 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.

#### 1.3. Background:

1.3.1. Statutory References: WV. Code §61-3C-3

1.3.2. MUBOG IT-1 policy replaced the original Computer Use and Abuse Policy, approved in 1995, and was 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.

#### 1.4. Definitions

1. "**Access**" means to instruct, communicate with, store data in, retrieve data from, intercept data from or otherwise make use of any computer, computer network, program, software, data or other resources.

2. "**Authorization**" means the express or implied consent given by a person to access or use said person's computer, computer network, program, software, system, password, identifying code or personal identification number.
3. "**Device**" means an electronic, magnetic, optical, or other device performing logical, arithmetic or storage functions and includes any data storage facility or communication facility directly related to or operating in conjunction with such device. The term "computer" includes any connected or directly related device, equipment or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device, file servers, mainframe systems, desktop personal computers, laptop personal computers, tablet personal computers, cellular telephones, game consoles and any other electronic data storage device or equipment, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator or other similar device.
4. "**Data**" means any representation of knowledge, facts, concepts, instruction or other information computed, classified, processed, transmitted, received, retrieved, originated, stored, manifested, measured, detected, recorded, reproduced, handled or utilized by a computer, computer network, computer program or computer software and may be in any medium, including, but not limited to, computer printouts, microfilm, microfiche, magnetic storage media, optical storage media, punch paper tape or punch cards, or it may be stored internally in read-only memory or random access memory of a computer or any other peripheral device.
5. "**Network**" means a set of connected devices and communication facilities, including more than one computer, with the capability to transmit computer data among them through such communication facilities.
6. "**Computer operations**" means arithmetic, logical, storage, display, monitoring or retrieval functions or any combination thereof and includes, but is not limited to, communication with, storage of data in or to, or retrieval of data from any device and the human manual manipulation of electronic magnetic impulses. A "computer operation" for a particular computer shall also mean any function for which that computer was designed.
7. "**Program, software or application**" means an ordered set of computer data representing instructions or statements, in a form readable by a computer, which controls, directs or otherwise influences the functioning of a computer or computer network.
8. "**Technology Services**" means access time, data processing or data storage and the data processed or stored in connection therewith.
9. "**Information Technology Resources**" includes, but is not limited to, information retrieval; computer data processing, transmission and storage; and any other functions performed, in whole or in part, by the use of a computer, computer network, computer software or computer program.
10. "**Owner**" means any person who owns or leases or is a licensee of a computer, network, data, program, software, resources or supplies.

## **2 Policy:**

### **2.1. Introduction**

Marshall University is 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 Technology resources available to faculty, staff, and students. These resources include educational, research, and communication facilities, disk storage, and selected software or services. 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 Resources.

### **2.2. General Principles and Guidelines**

The basic premise of this policy is that responsible and acceptable use of the Marshall University Information Technology Resources 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 Information Technology Resources were 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 Information Technology Resources, or University sponsored remote resources, are those individuals who have been granted a username and password. The username and password combination is the users' identity and authorization to access and use the components of the Marshall University Information Technology Resources for which they 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 Information Technology Resources are finite and shared. Appropriate and responsible use of these resources must be consistent with the common good. These resources may NOT be used for individual gain or personal profit-making purposes.
- 2.2.5. The University reserves the right to limit access to the Marshall University Information Technology Resources 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 Information Technology Resources. Use of the Information Technology Resources is a privilege, therefore the University reserves the right to restrict or deny usage of the Information Technology Resources 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 as explained in the administrative procedure ITP-1. Marshall University Copyright Procedure.
- 2.2.8. Web pages hosted on university resources may NOT contain the official Marshall University logo unless it is according to the University Communications Branding guidelines.
- 2.2.9. "Mass Mailings" are excessive, unauthorized, and frivolous mailings of two hundred or more identical or nearly identical pieces of electronic communication sent by a user or users to other email or voice recipients and not allowed without approval. The details for approval are found in MUBOG IT-3 Electronic Communications Policy.
- 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;

- 2.2.12. Connecting unauthorized equipment to the campus network or computers. 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 ports, routers, switches, wiring, and connections;
- 2.2.14. Utilizing network or system identification numbers or names that are not assigned for one's specific use on the designated system;
- 2.2.15. Registering a Marshall University owned IP address with any other domain name without authorization is prohibited.
- 2.2.16. Using campus resources to gain unauthorized access to any computer system and/or using someone else's device without their permission or access based on their job description;
- 2.2.17. Providing services or accounts on University computers or via University networks to other users unless required to meet the normal activities of students working as individuals or in collaborative groups to fulfill current course requirements. University authorized business and other activities directly related to the academic mission of the University are also excluded; however, any computers running services that may negatively impact management, reliability or integrity of the campus network or other University resources may be disconnected from the network;
- 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.

### **3 Non-Compliance and 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 Office of the Chief Information Officer (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.

### 3.1. Common Forms of Violations

Although most users strive for acceptable and responsible use of the Information Technology Resources, 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.

- 3.1.1. Furnishing false or misleading information or identification in order to access another user's account
- 3.1.2. Using another person's username/password or letting someone else use your username/password
- 3.1.3. Investigating, reading or attempting to access another user's files without permission
- 3.1.4. Attempts to access or manipulate certain components of the Information Technology Resources without authorization
- 3.1.5. Alteration of software, data, or other files without authorization
- 3.1.6. Disruption or destruction of equipment or resources
- 3.1.7. Using subterfuge to avoid being charged for computer resources or deliberate, unauthorized use of another user's account to avoid being billed for services
- 3.1.8. Using, copying or distributing copyrighted works or software without authorization
- 3.1.9. Sending email or a program which will replicate itself or may cause damage to another user's account
- 3.1.10. Interfering with legitimate work of another user
- 3.1.11. Sending abusive, harassing, or obscene messages
- 3.1.12. Viewing or listening to objectionable, obscene, pornographic, or harassing material in public areas
- 3.1.13. Excessive recreational use of resources
- 3.1.14. Sending unauthorized mass mailings, chain letters, or transmitting a crippling number of files across a network
- 3.1.15. Sending hoax messages or forged messages, including messages sent under someone else's username
- 3.1.16. 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.

### 3.2. Enforcement

Information Technology is authorized to engage in investigations and apply certain penalties to enforce this policy. These penalties include, but are not limited to, temporary or permanent reduction or elimination of access privileges to any or all of the components of the Information Technology Resources. If, in the opinion of Information Technology, it is necessary to preserve the integrity of facilities, services, or data, IT may suspend any access, whether or not the account owner is suspected of a violation. In such a case, IT will attempt to notify the user of any such action after the potential threat to the facilities, services, or data is contained. If such an investigation is required it will be done only under the direct authorization of the Chief Information Officer (CIO) and all effort will be made not to disclose any content to anyone other than those with a need to know during the investigation or adjudication of the alleged offense

Consequences of the discovery and investigation process or normal maintenance might include the inspection of files contained in an individual's storage space or monitoring selected traffic on the

networks. Again, all effort will be made not to disclose any content to anyone other than those with a need to know. However, where there are moral, ethical, or legal implications of the nondisclosure of such information, Information Technology personnel are similarly instructed to contact the Chief Information Officer (CIO) (CIO@marshall.edu), who may authorize its disclosure to appropriate authorities if deemed warranted.

In most cases an individual accused of a violation of this policy will be notified and have an opportunity to respond before a final determination of a penalty is made. The Chief Information Officer (CIO) or their designee, in conjunction with other responsible parties (e.g., University General Counsel, Student Affairs, Academic Affairs, or Human Resources) will examine the available evidence and circumstances. If a penalty is levied, the decision may be appealed through the appropriate channels.

#### **4 Related Policies, Administrative procedures and Guidelines**

4.1. Administrative Procedure ITP- 23 Password Standards

4.2. Family Educational Rights and Privacy Act (FERPA)