MARSHALL UNIVERSITY INFORMATION TECHNOLOGY COUNCIL

Standard ITP-44

Standard for Security of Information Technology Resources

1. General Information:

Marshall University expects all individuals using information technology devices connected to the Marshall University Network (MUNet) to take appropriate measures to manage the security of those devices. In addition, the University establishes roles and responsibilities surrounding the technical procedures required for the security of these devices.

1.1. Scope: Marshall University and all units that are directly associated with the institution. All members of the University community

1.2. Authority: W. Va. Code §18B-1-6, MUBOG IT-1, MUBOG IT-2

1.3. Passage Date: January 8, 2016

1.4. Effective Date: January 8, 2016

1.5. Last Revised: August 19, 2019

1.6. Related Policies, Procedures and Guidelines:

University Policies and Documents
University Board of Governor Policies
University Guideline ITG-4 Guidelines for Data Classification
University Procedure ITP-27 Information Security Roles and Responsibilities
University Policy IT-2 Information Security Acceptable Use Policy
University Procedure ITP-19 Information Security Incident Response Procedure
University Procedure ITP-27 Information Security Roles and Responsibilities
University Code of Conduct Classified Staff Handbook
University Policy SA-3 Code of Student Rights and Responsibilities
Information Technology Securing your Computer

External Documentation

West Virginia Code S18B-1-6. Rulemaking.

Federal Student Aid DCL: GEN-15-18

West Virginia Code S61-3C. West Virginia Computer Crime and Abuse Act.

2. Purpose of Standard

The University must preserve its information technology resources, comply with applicable laws and regulations, and comply with other University or unit policy regarding protection and preservation of data. Given the distributed nature of information technologies and complexity of managing the security of information technology devices, the University wishes to set forth a foundation for the alignment of roles and responsibilities with regard to specific technical procedures.

3. Contacts – Marshall University Campus Units

Direct any general questions about this standard to your college or unit administrative office. If you have questions about specific issues, contact the following offices.

Subject	Contact	Telephone	E-mail/Web Address
Initial Contact for Questions	Local support provider	Unit-specific	
Policy Clarification	Chief Information Officer	(304) 696-3900	cio@marshall.edu www.marshall.edu/it/governance
Best Practices for Configuring and Securing IT Devices	Chief Information Security Officer	(304) 696-3270	infosec@marshall.edu www.marshall.edu/it/departments/information-security/
Computers and Network Systems	Chief Information Officer	(304) 696-3900	cio@marshall.edu www.marshall.edu/it/departments/computing-services/
Legal Issues	Office of University Counsel	(304) 696-6444	www.marshall.edu/president/
Security of Network Systems	Director of IT Infrastructure Communications	(304) 696-3209	itic@marshall.edu www.marshall.edu/it/departments/computing-services/

4. Definitions

Refer to ITP-10 for Terms and Definitions.

Responsibilities – Marshall University Campus Units

The major responsibilities each party has in connection with this policy are as follows:

Chief Information Security Officer	**Develop a comprehensive security program that includes risk assessment, best practices, education, and training.** **Identify, analyze, resolve, and report Marshall electronic security incidents.** **Assist or lead electronic security incident resolution for the University and individual units, and specifically in the Information Security Incident Response Team (ISIRT) process.** **Issue critical security notices to unit heads and security liaisons. Develop, implement, and support University-level security monitoring and analysis.** **Support and verify compliance with federal, state, and local legislation.**
Local Support Provider	Maintain knowledge of information technology (IT) devices under his or her control through identification and understanding of their usage. Follow safe security practices when administering IT devices under his or her control. Follow electronic security incident reporting requirements in accordance with University ITP-19 Information Security Incident Response Procedure.
Unit Head	Assume final responsibility for the security of IT devices within his or her unit. Identify a security liaison. Implement unit security programs consistent with this policy.
Unit IT Manager	Consult with the Chief Information Officer (CIO) regarding campus IT issues
Unit Security Liaison	Act as the unit point of contact with Chief Information Security Officer. Implement a security program consistent with requirements of this standard (for example, the implementation of risk assessment, best practices, education, and training) and in keeping with the specific IT security needs of his or her unit. Act as the security coordinator for the local support providers (in units where the unit security liaison is not the local support provider). Implement unit procedures and protocols for the reporting of electronic security incidents in accordance with University ITP-19 Information Security Incident Response Procedure. Work with the unit head, IT manager, director, and other relevant personnel to address critical security notices issued by the Chief Information Security Officer or his or her staff.
User **User (cont.)**	Comply with the current policies, requirements, guidelines, procedures, and protocols concerning the security of the University's electronic networks and devices. *(continued next page)* Protect IT resources under his or her control with measures such as the responsible use of secure passwords, appropriately establishing an administrator password, and timely antivirus updates. Assist in the performance of remediation steps in the event of a detected vulnerability or compromise.

	Comply with directives of University officials, such as the Chief Information Security Officer and his or her delegates, to maintain secure devices attached to the network regarding software patches and/or virus protection. Take note of circumstances in which he or she may assume the responsibilities of a local support provider, e.g., by attaching a personal computer to the Marshall University network or working remotely from home. Follow electronic security incident reporting requirements in accordance with University ITP-19 Information Security Incident Response Procedure.

5. Principles

5.1. Introduction - In order to manage information technology (IT) security comprehensively, this standard serves five major purposes.

5.1.1. It establishes the principle that every IT device connected to the Marshall University network must have at least one individual managing the security of that device.

5.1.2. It requires Units to designate Unit Security Liaisons (see the *Obligations of the Unit Security Liaison* segment of procedures).

5.1.3. It creates the following five categories of individuals, each with specific obligations regarding the security of IT devices:

5.1.3.1. User

5.1.3.2. Local support provider

5.1.3.3. Unit security liaison

5.1.3.4. Unit head

5.1.3.5. Chief Information Security Officer

5.1.4. It delineates specific responsibilities for each category of user.

5.1.5. It creates the foundation for the University's administrative approaches to IT security by aligning roles and responsibilities with technical procedures.

♦Note: All users of IT devices must follow the procedures outlined in the *Obligations of Users* section of procedures.

♦Note: The focus of this standard is on the security of IT devices and resources, and not on specifics for the management of data or any particular class of data. For information concerning data, please consult University Guideline ITG-4 Guidelines for Data Classification, which provides the authority for and guidance towards the development of policy for the preservation and proper management of data in specific functional areas.

♦Note: As a foundational standard, this document relies on other university policies; see Related Resources for more information about those policies.

5.2. Procedures – Marshall University Campus Units

5.3. Obligations of the User –

Any individual who uses an information technology (IT) device (see the definitions section of this document) is a user. Each of these devices may or may not have a local support provider assigned to it. Users have different obligations, based upon whether a local support provider has been assigned to a particular device.

Typically, University-owned IT devices located in campus workspaces have local support providers assigned to them. On the other hand, personally-owned computers used to connect to the Marshall University network from any location (home, off campus, residence hall or other on-campus location) usually do not.

♦Note: If you cannot perform or do not understand any of the obligations assigned to users, contact the Marshall University IT Service Desk, at ITServiceDesk@marshall.edu.

5.4. Obligations of a User Whose Device DOES Have a Local Support Provider

5.4.1. Understand and comply with current policies, requirements, guidelines, procedures, and protocols concerning the security of the University's electronic networks and devices (see the related documents section of this document).

5.4.2. Comply with guidelines and practices established by the local support provider for the IT device.

5.4.3. Contact your local support provider whenever a questionable situation arises regarding the security of your IT device.

5.4.4. Report all electronic security incidents to your local support provider immediately, as detailed in University ITP-19 Information Security Incident Response Procedure.

5.5. Obligations of a User Whose Device DOES NOT Have a Local Support Provider

(*If you cannot perform or do not understand any of the obligations below, contact the Marshall University IT Service Desk, at ITServiceDesk@marshall.edu)*

5.5.1. Understand and comply with current policies, requirements, guidelines, procedures, and protocols concerning the security of the University's electronic networks and IT devices (see the related documents section of this document).

5.5.2. Update campus-wide security applications, including antivirus software and operating system updates, in a timely fashion.

5.5.3. Protect the resources under your control with the responsible use of secure passwords and by appropriately establishing an administrator password.

5.5.4. Assist in the performance of remediation steps in the event of a detected vulnerability or compromise.

5.5.5. Comply with directives of university officials, such as the Chief Information Security Officer, unit security liaison, or local support provider(s), to maintain secure devices attached to the network.

5.5.6. Follow electronic security incident reporting requirements in accordance with University ITP-19 Information Security Incident Response Procedure.

5.6. Obligations of a Local Support Provider

A local support provider is the individual with principal responsibility for the installation, configuration, and ongoing maintenance of an IT device (e.g., system administrator or network administrator). A local support provider seeking guidance or clarification should contact his or her unit security liaison or the Chief Information Security Officer.

The local support provider is responsible to do the following:

5.6.1. Be knowledgeable and comply with the current policies, requirements, guidelines, procedures, and protocols concerning the security of the University's IT resources.

5.6.2. Follow appropriate best practices guidelines for configuring and securing IT devices. See www.marshall.edu/it/departments/information-security/computer-safety-tips/

5.6.3. Understand and document the specific configurations and characteristics of the IT devices he or she supports to be able to respond to emerging IT threats and to support security event mitigation efforts appropriately.

5.6.4. Understand and recommend the appropriate measures to provide security to the resources under his or her control, including, but not limited to the following:

5.6.4.1. Physical security to protect resources such as keys, doors, and/or rooms maintained to the level of security commensurate with the value of the resources stored in those locations.

5.6.4.2. Administrative security to protect resources such as:

- Full implementation of the most current authentication and authorization technologies utilized by the architecture of the University network and/or its technology resources.
- The most recently tested and approved software patches available.
- The most contemporary and available security configurations.
- The most contemporary and available virus protection.
- Configuration of secure passwords on all IT devices (eliminating all default or administrative passwords).

5.6.5. Follow electronic security incident reporting requirements in accordance with University ITP-19 Information Security Incident Response Procedure.

♦Note: Local support providers should be mindful of potential responsibilities they may have as custodians of administrative data transmitted or stored on IT devices under their control. Please consult University Guideline ITG-4 Guidelines for Data Classification, for further guidance.

5.7. Obligations of the Unit Security Liaison

The Unit Security Liaison is the person designated by the Unit Head as the primary contact for the Chief Information Security Officer. For further guidance or clarification, contact the Chief Information Security Officer.

The unit security liaison is responsible to do the following:

5.7.1. Act as the unit point of contact with the Chief Information Security Officer.

5.7.2. Implement a security program consistent with the requirements of this standard (for example, the implementation of security assessment, best practices, education and training), consistent with University guidelines and practices and in keeping with the specific IT security needs of his or her unit. This will include the following:

5.7.2.1. Identify the IT resources under his or her control.

5.7.2.2. Oversee compliance with all IT security regulations under federal, state, and local law.

5.7.2.3. Provide proper information and documentation about those resources.

5.7.2.4. Participate in and support security risk assessments of his or her IT resources, including the following:

5.7.2.5. The degree of sensitivity or importance of the data transmitted or stored on those resources.

5.7.2.6. The criticality of its connection to the network and a continuity plan in the event that it must be disconnected or blocked for security reasons.

5.7.2.7. The vulnerability of a particular resource to be used for illegal or destructive acts.

5.7.2.8. The vulnerability of a particular resource to be compromised.

5.7.2.9. The plan to be followed in the event of disaster for recovery.

5.7.2.10. The measures routinely taken to ensure security for each device.

5.7.3. Act as the security coordinator for the local support provider(s) within his or her unit (in units where the unit security liaison is not the local support provider) including the following:

5.7.3.1. Developing intermediate and harmonizing processes between University and unit policy and procedure.

5.7.3.2. Assisting the IT Security Office in the investigation of security issues and incidents, and, in the case of a loss or breach of institutional data and information, representing the unit in the Information Security Incident Response Team (ISIRT) process.

5.7.3.3. Disseminating information and communications about security policy, procedures, and other information from the IT Security Office to users within the unit.

5.7.4. Implement unit procedures and protocols for the reporting of electronic security incidents in accordance with University ITP-19 Information Security Incident Response Procedure.

5.7.5. Work with the unit head, the unit IT manager, director and/or other relevant personnel to address critical security notices issued by the Chief Information Security Officer or his or her staff.

♦Note: The unit security liaison may want to take specific measures toward the protection of data stored or transmitted on the IT devices under his or her management and/or be mindful of any potential responsibilities as custodians of administrative data. Please consult with University Guideline ITG-4 Guidelines for Data Classification, for guidance.

5.8. Obligations of the Unit Head

Unit heads or individuals with responsibility for administrative units (e.g., vice presidents of administrative units, deans, department heads, etc.) have overall, local responsibility for the security of IT resources under their control. For further guidance, contact your unit security liaison or the Chief Information Security Officer.

The unit head's oversight responsibilities in relation to security IT resources include, but are not limited to, the following:

5.8.1. Identify a unit security liaison to the Chief Information Security Officer, who may in some cases also be the local support provider (depending upon the size of the unit and discretion of the unit head).

5.8.2. Ensure that, through the unit security liaison, a security program is implemented for the unit consistent with requirements of this standard (for example, the implementation of security assessment, best practices, education and training), consistent with University guidelines and practices and in keeping with the specific IT security needs of his or her unit.

5.8.3. Provide administrative control over continuity of support over all the IT devices in the unit such that, for example, a change in employment of an individual local support provider does not result in the abandonment of responsibility over IT devices attached to the network.

5.8.4. Oversee the creation and implementation of procedures for the reporting of electronic security incidents in accordance with University ITP-19 Information Security Incident Response Procedure.

♦Note: Unit heads may want to take specific measures toward the protection of data stored or transmitted on the IT devices under their management. Please consult with University Guideline ITG-4 Guidelines for Data Classification, for guidance.

5.9. Obligations of the Chief Information Security Officer

The Chief Information Security Officer is the University officer with the authority to coordinate campus IT security. The following are obligations of the Chief Information Security Officer:

5.9.1. Develop a comprehensive security program that includes risk assessment, best practices, education, and training.

5.9.2. Strive for proper identification, analysis, resolution, and reporting of Marshall electronic security incidents; assist or lead electronic security incident resolution for the University and individual units, specifically in the Information Security Incident Response Team (ISIRT) process.

5.9.3. Issue critical security notices to unit heads and security liaisons.

5.9.4. Develop, implement, and support University-level security monitoring and analysis.

5.9.5. Support and verify compliance with federal, state, and local legislation.

6. Violations

Legitimate use of a computer or network system does not extend to whatever an individual is capable of doing with it. Although some rules are built into the system itself, these restrictions cannot limit completely what an individual can do or can see. In any event, each member of the community is responsible for his or her actions, whether or not rules are built in, and whether or not they can be circumvented. It is an explicit violation of this standard to do any of the following:

6.1. Knowingly or intentionally maintain insecure passwords on IT devices attached to the network (e.g., absence of administrative password, password written and stored in insecure location, shared passwords, etc.).

6.2. Knowingly or intentionally attach misconfigured IT devices to the network.

6.3. Knowingly or intentionally compromise an IT device attached to the network or intentionally use an application or computing system with a known compromise.

6.4. Knowingly or intentionally, (or negligently after receiving notice from an IT officer or professional), transmit any computer virus or other form of malicious software.

6.5. Knowingly or intentionally access or exploit resources for which you do not have authorization.

6.6. Knowingly or intentionally perform network or system scans on resources not authorized by the Chief Information Security Officer, unit head, unit security liaison, or local support provider.

7. Enforcement

Suspected violations will be investigated by the appropriate office, and disciplinary actions may be taken in accordance with the Campus Code of Conduct, applicable regulations, or other University policy.

7.1. Reporting Suspected Violations

All violations of this standard must be reported to the Chief Information Security Officer. The Chief Information Security Officer will refer these cases for disciplinary action to the following officers:

7.1.1. If the alleged violator is a student, the Office of Student judicial administrator.

7.1.2. If the alleged violator is a non-academic employee, the Office of Human Resources.

7.1.3. If the alleged violator is an academic employee, the Division of Academic Affairs.

Source: ITP-44 Security of Information Technology Resources is modeled after the following policy:
https://www.dfa.cornell.edu/sites/default/files/policy/vol5_4_1_0.pdf