Board of Governors Rule

Governance
Information Technology Resources
Responsible Unit: Academic Affairs/
Information Technology Services
Adopted: February 8, 2019
Effective: March 1, 2019
Revision History: Prior BOG Policy #54
(Originally effective January 29, 2010)
Review Date: February 2023

BOG GOVERNANCE RULE 1.11
INFORMATION TECHNOLOGY RESOURCES AND GOVERNANCE

SECTION 1: PURPOSE & SCOPE.

1.1 The Board of Governors ("Board") seeks to outline the guiding principles for using, securing, and maintaining Information Technology Resources.

1.2 This Rule applies to all West Virginia University staff, faculty, students, and volunteers, as well as any third-party individuals and entities, who access the Information Technology Resources of West Virginia University. The Rule also applies to West Virginia University, West Virginia University Institute of Technology and Potomac State College of West Virginia University (collectively the "University").

SECTION 2: DELEGATION TO PRESIDENT OF INFORMATION TECHNOLOGY POLICIES AND PROCEDURES.

2.1 ***Delegation.*** To enable the University to function in a proper, expeditious, and secure manner and to advance the University's mission and objectives, the Board delegates to the President the following authority to establish and maintain a framework for the routine review and implementation of policies and procedures aimed at creating a rich, integrated, compliant, and secure electronic environment in which to educate students, engage in research, perform outreach services, and conduct the University's business.

2.2 ***Reporting.*** At least annually, the Board shall be provided with an update on matters relating to the deployment of Information Technology Resources and information security; provided, however, that the Chair of the Board shall promptly be notified of any significant Information Security Event.

SECTION 3: INFORMATION TECHNOLOGY GOVERNANCE.

3.1 There shall be framework for governance and compliance within the University that, at a minimum:

3.1.1 Provides reliable Information Technology Resources that are readily available for use by Authorized Users in accordance with an established acceptable use policy.

3.1.2 Establishes guidelines for the responsible management of University-owned Information Technology Resources including the purchase, inventory, and replacement of such resources.

3.1.3 Safeguards the confidentiality and integrity of Information Technology Resources from unauthorized access, loss, alteration, or damage while also supporting the open, information-sharing needs of our academic culture.

3.1.4 Establishes information security and risk management strategies that outline an efficient and effective process for responding to an Information Security Event.

3.1.5 Provides awareness and training materials to the University community regarding information privacy and security policies, standards, guidelines, and best practices, including notifying Authorized Users that there is no expectation of privacy when using Information Technology Resources which are owned or controlled by the University.

3.1.6 Provides for the security and privacy of University data in accordance with applicable laws and definable information technology security standards.

3.1.7 Implements a prevention program that is documented in writing and designed to identify and detect the warning signs ("red flags") of Identity Theft in day-to-day operations.

3.18 Fosters effective collaboration within the University to efficiently provide Information Technology Resources and technical support that aligns with up-to-date technologies, trends, and issues.

3.2 All information technology policies and procedures shall be consistent with Federal and State law and any Rule adopted by the Board of Governors.

SECTION 4: ENGAGEMENT WITH UNIVERSITY COMMUNITY AND OVERSIGHT

4.1 Where appropriate, the President is encouraged to seek input from the University community through formal committees as well as other informal efforts regarding the development and implementation of information technology policies and procedures.

4.2 The President shall establish an appropriate framework for oversight and enforcement of information technology policies and procedures.

4.3 At least once every three years, a comprehensive review of the University's information technology policies and procedures should be undertaken. To conduct such a review, the University may involve external consultants.

SECTION 5: DEFINITIONS.

5.1 "Authorized Users" means faculty, staff, students, volunteers, and other third parties who have been granted access via WVU Login credentials to the University's Information Technology Resources.

5.2 "Information Security Event" means any real or suspected event that may adversely affect the availability and security of the University's Information Technology Resources that support academic, administrative, or research operations.

5.3 "Identity Theft" means fraud committed or attempted using identifying information of another person without authorization.

5.4 "Information Technology Resources" means hardware, software, and communications equipment, including, but not limited to, computers, email, internet, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, facsimile machines, technology facilities (including but not limited to: data centers, dedicated training facilities, and switching facilities), and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

5.5 "President" means the President of the University or the President's designee.

SECTION 6: AUTHORITY.

6.1 W.Va. Codes §18B-1-6, § 18B-2A-3, and 15 U.S.C. 1681 et seq. and its implementing regulations 16 CFR Part 681.

SECTION 7: SUPERSEDING PROVISIONS.

7.1 This Rule supersedes and replaces any rule of the Higher Education Policy Commission which relates to the subject matter contained within this Rule. This Rule also repeals and supersedes WVU BOG Policy 54 – Rule on Identity Theft Detection and Prevention Program adopted January 29, 2010, and any other internal University policy or procedure which relates to the subject matter contained within this Rule.