Approval Date: October 14, 2020
Effective Date: October 14, 2020
Revision History:
President's Signature: On file

SECTION 1: Purpose and 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 Liberty University staff, faculty, students, volunteers and guests, as well as any third-party individuals and entities, who access the Information Technology Resources of West Liberty University.

SECTION 2: Delegation to President

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.

3.1.8 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: Definitions

4.1 "Authorized Users" means faculty, staff, students, volunteers, guests, and other third parties who have been granted access via WLU Login credentials or via WLU Guest Wireless Network to the University's Information Technology Resources.

4.2 "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.

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

4.4 "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.

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

SECTION 5: Authority

5.1 W.Va. Code §18B-1-6

SECTION 6: Superseding Provisions

6.1 This Rule repeals and supersedes WLU BOG Policy 49 – Computer Abuse adopted December 11, 2006 and any other internal University policy or procedure which relates to the subject matter contained within this Rule.