1.0 PURPOSE and SCOPE

It is the policy of the State University of New York College at Old Westbury (the College) to establish policies, standards and procedures for access and proper use of the College's E-mail System, the Internet and Computer Resources. This policy applies to all Computer Users at the College.

2.0 DEFINITIONS

2.1 CHIEF INFORMATION OFFICER: The College official responsible for providing computing, telecommunications technology and information technology services to the campus.

2.2 INTERNAL CONTROL OFFICER: The College official responsible for reviewing and reporting on the College's program of internal controls, including policies and procedures, in accordance with the NYS Governmental Accountability, Audit and Internal Control Act.

2.3 INTERNET SECURITY OFFICER: The College official who oversees and coordinates the implementation of policies governing security and privacy on Internet and email-related matters.

2.4 INTERNET SERVICES PROVIDER: An entity that has a physical connection to the Internet and that provides persons and entities with an electronic link to the Internet. The Internet Services Provider for the College is designated by the Chief Information Officer to provide the College with access to the Internet and other services in connection with such access, and that is or shall be providing such access and performing such services for the College pursuant to contract.

2.5 COLLEGE STANDARDS AND PROCEDURES: Standards and procedures that currently exist or may be adopted in the future, as the same may be modified, amended or supplemented.

2.6 COMPUTER RESOURCES: All computers, including laptops and other portable computing devices and all related peripheral equipment, servers, data storage devices, communications networks, and software owned by, contracted for, or under the control of the College at any location.

2.7 COMPUTER USER: Any user of Computer Resources, including employees, temporary employees, consultants, contractors, students and guests.

2.8 FIREWALL: An electronic barrier placed between two or more networks that is used to screen or restrict electronic communications between or among networks.

2.9 COMPUTING SERVICES: The central organizational unit within the College responsible for providing computing, telecommunications and information technology services.

2.10 RESTRICTED OR PROHIBITED INTERNET SITE: Any Internet site designated by the College's Chief Information Officer or designee as restricted or prohibited. A site does not need to be specifically designated as restricted or prohibited to be a Prohibited Internet Site. For purposes of this policy, it is sufficient that a site is included within a general description of prohibited or restricted sites to be considered a Prohibited Internet Site.

3.0 RESPONSIBILITIES

3.1 Computing Services is responsible for the general administration of this policy and any applicable College standards and procedures. Computing Services shall communicate this policy and all specific standards and procedures to those Computer Users who have received approval to access or use the Internet via a College Computer Resource.

3.2 Each Vice President and Division Head is responsible for ensuring that employees and other Computer Users within his/her division adhere to this policy and applicable College standards and procedures. Upon receipt of requests for information deemed actionable, each Vice President should consult with the campus Internet Security Officer to determine further action.

3.3 Each Computer User is responsible for adhering to this policy and complying with all applicable College rules and policies.

3.4 The Internal Control Officer or designee shall periodically perform reviews to determine compliance with this policy and applicable College standards and procedures.

4.0 INTERNET ACCESS

4.1. EDUCATIONAL AND BUSINESS USE

The Internet offers access to vast amounts of information on varied topics. The College's primary purpose in providing access to the Internet is to facilitate its educational, research and business purposes. The College encourages the appropriate and responsible use of the Internet to assist Computer Users in the performance of their jobs, enhancement of their education and in the furtherance of legitimate College purposes.

4.2 INCIDENTAL PERSONAL USE

A Computer User may not access or use the College's E-mail System or the Internet via a Computer Resource for incidental personal use if such use:

a) is in furtherance of a non-College business enterprise;
b) interferes with the Computer User's employment obligations;
c) promotes charitable, religious, political, or personal preferences and activities that benefit the external unit or individual; and
d) is not in compliance with all applicable policies, standards and procedures including, but not limited to this Internet Security Policy.

The incidental personal access or use of the Internet via a Computer Resource is at the sole risk of the Computer User and the College has no responsibility for any technical malfunctions or damages associated therewith.

4.3. AUTHORIZATION FOR INTERNET ACCESS

Only authorized Computer Users under this policy are allowed access to the College's Computer Resources, including the Internet. The College's Chief Information Officer or designee may prevent, based on security or legitimate business concerns, in whole or in part, any Computer User from accessing or using the Internet at anytime without notice.

4.4 COLLEGE APPROVED INTERNET SERVICES PROVIDER

Access to the Internet shall be via a College-Approved Internet Services Provider unless a Computer User has received specific permission in accordance with College standards and procedures, to use another Internet Services Provider. Any unauthorized use of or access to the Internet via a non-approved Internet Services Provider is prohibited. The provision of unauthorized Internet computer services by students using the campus network is also prohibited.

4.5 PROPER COMMUNICATIONS

All communications and activities involving the College's E-Mail System and the Internet must be professional, lawful, ethical and in accordance with College policies and standards. The College's policies prohibiting unlawful discrimination and harassment apply fully to access to and use of the Internet. Care should be taken when transmitting communications containing privileged, confidential, proprietary or personal information. The College's Computing Services shall establish and implement procedures for protecting the transmission and receipt of such communications over the Internet including, but not limited to, the following: to use encryption technology, if appropriate and available; to assure that transmission is for a legitimate College purpose and is pursuant to appropriate authorization; and to ensure that the recipient is authorized to receive such information.

4.6 ELECTRONIC DATA TRANSFER TO NON-COLLEGE SYSTEMS

The distribution or receipt of software, data, or other materials via the Internet, computer based on-line services or other electronic messaging systems, must be in accordance with this policy and any applicable College standards and procedures. The College's Computing Services shall establish standards for the designation and use of file transfer protocols to provide for the transfer of files or data to and from another network or system.

4.7 PROHIBITED ACTIONS

To ensure the integrity of College Computer Resources, protect confidential and proprietary information and comply with applicable laws, the following actions are prohibited:

a) connection to or viewing of a Prohibited Internet Site;
b) connection to any Internet site for the purpose of viewing, downloading, transmitting or printing material that is fraudulent, obscene, threatening, defamatory, harassing, or relates to unauthorized hacking; connection to the Internet for purposes of solicitation or proselytizing for charitable, religious, political or other non-College business purposes or for personal profit, unless such actions are approved in accordance with applicable College policies, standards and procedures;
c) connection to the Internet via an Internet Service Provider that has not been approved in accordance with this policy and applicable College standards and procedures;
d) downloading, installation or storage of software that is not approved in accordance with applicable policies and College standards and procedures;
    1) transmission, use or storage of any material or information in violation of applicable trademark, patent and copyright laws and/or license agreements;
    2) actions that attempt to disable, defeat or circumvent any security features or monitoring,

including but not limited to security firewalls and file transfer protocols.

3) accessing campus administrative system over the wireless network.

Each Computer User must take appropriate measures to protect against unauthorized access to the campus network and Internet, e.g. no person should leave sessions open and unattended or share authentication identifications used to log on to the Internet.

If you become aware of the commission of any of the actions described in this section (4.7a – d) or any other action which you believe is prohibitive in nature, contact the Internet Security Officer.

4.8. NO EXPECTATION OF PRIVACY; COLLEGE RIGHTS TO MONITOR, ACCESS AND REVIEW

Upon written authorization by the College President, the Internet Security Officer or others working on behalf of the College President, can initiate action to monitor and review information under this policy. By using Computer Resources, including the Internet, the Computer User:

a. understands there is no expectation of privacy with respect to the messages, files, data or other information, including, without limitation, e-mail and Internet use and usage records, on or transmitted through the Computer Resources, regardless of whether such messages, files, data or other information is identified as personal, private, confidential or otherwise, and
b. consents to the College's unconditional right in furtherance of its legitimate business purposes, without notice to the Computer User, to monitor, access, review, inspect, copy, delete and/or disclose such messages, files, data, and other information.

Passwords and encryption software are provided solely for the benefit of the College and should not be misconstrued as a means of protecting the privacy of electronic communications.

5.0 NETWORK SECURITY

5.1 FIREWALL

The College has its own direct link to a College-Approved Internet Services Provider and shall ensure that it has, at all times, a Firewall in place. The College's Chief Information Officer shall ensure that the Firewall is appropriately configured and monitored on an on-going basis to ensure network security.

5.2 ACCESS TO DATA

The College shall establish and enforce standards and procedures that will ensure that all data residing on the College's systems and networks are properly protected against unauthorized access.

5.3 NETWORK INTEGRITY

All changes or additions to the College network configuration must be approved by the Computing Services. No Computer User shall alter any College network configuration without the prior approval of Computer Services.

6.0 VIOLATION

Individuals or groups found in violation of this policy will undergo appropriate disciplinary procedures, including campus or legal proceedings, where appropriate.

7.0 AUTHORIZATION

This Policy has been adopted by the College's Technology Steering Committee. It was reviewed by the Internal Control Officer, the Chief Financial Officer and the Assistant to the President for Administration prior to approval by the President.