I. POLICY 1

II. PURPOSE AND SCOPE.....1

III. RESPONSIBILITIES 1

IV. DEFINITIONS.....1

V. PROCEDURES 2

VI. PRIVACY 6

VII. ENFORCEMENT AND EXCEPTIONS 6

VIII. REFERENCES.....7

IX. APPROVALS 7

I. POLICY

It is the mission and the established practice of SUNY Old Westbury to provide employees and students access to electronic information and services, computing facilities, networks and other technology resources. Activities related to the College's mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the College's mission is prohibited.

This policy respects privacy rights of the College's constituents including the right of employees to be free from intimidation, harassment, and unwarranted annoyance. All users of College's computing resources must adhere to the requirements and procedures of this policy.

II. PURPOSE AND SCOPE

SUNY Old Westbury's technology infrastructure exists to support the institutional and administrative activities needed to fulfill the College's mission. Access to these resources is a privilege that should be exercised responsibly, ethically and lawfully. This policy delineates the role each employee plays in protecting the College's information assets and outlines the minimum expectations for meeting these requirements. Fulfilling these objectives will enable the College to implement a comprehensive system-wide Information Security Program.

This policy applies to all users of computing resources that are owned, managed or otherwise provided by SUNY Old Westbury. Individuals covered by this policy include, but are not limited to all workforce employees and service providers with access to the College's computing resources or facilities. Computing resources include all College owned, licensed or managed hardware and software, E-mail domains, and other services. This policy also applies to any use of the College's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

III. RESPONSIBILITIES

All College users are responsible for any activity originating from their user account which they can reasonably be expected to control. In cases when unauthorized use of accounts or college technology resources is detected or suspected, the end user should change the password of the account and report the incident to Information Technology Services (ITS) Service Desk.

The College's *Chief Information Officer (CIO*) is responsible for providing college technology resources and information technology services to the campus. The CIO or designee, in consultation with the Senior Vice President of Business & Finance, may prevent, based on security or legitimate business concerns, in whole or in part, any User from accessing or using the Internet or college systems at any time, without notice. The College's *Information Security Officer (ISO)* is responsible for overseeing and coordinating the implementation of college policies governing security and privacy on Internet and E-mail-related college matters. Users should consult with the ISO if there are questions regarding the Internet, college systems and E-mail security related matters.

Questions as to how the various laws, rules and regulations may apply to a particular use of college technology resources should be forwarded to the CIO. Legal questions should be forwarded to the College's *Assistant to the President for Administration*.

IV. DEFINITIONS

College Technology Resources – (1) college owned, operated, leased or contracted computing, networking, Email, telephone and information resources, whether they are individually controlled, shared, standalone or networked; (2) information maintained in any form and in any medium within college technology resources, and (3) college voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities, including all hardware

(desktop computers, laptops, portable handheld computing devices, "smartphones", etc.), software, applications, databases, and storage media. Additionally, all creation, processing, communication, distribution, storage, and disposal of information by any combination of college technology resources and non-college technology resources are covered by this policy.

Incidental Personal Use – minimal or occasional use of college technology resources by user which does not result in any measurable cost or distraction to the College and benefits the College by allowing personnel to avoid needless inconvenience. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's responsibilities, or adversely impact or conflict with activities supporting the mission of the College.

User Account – an established relationship between a user and a computer, network or information service. Use of the College's computer systems and network requires that a user account be issued by the College. The user account is the responsibility of the person in whose name it is issued. College recognized clubs and student organizations may be issued a user account. Faculty advisors shall designate a particular person(s) authorized to act on behalf of the club or organization. This person(s) is responsible for all activity on the account and will be subject to College disciplinary procedures for misuse.

V. PROCEDURES

A. Fraudulent and Illegal Use – The College explicitly prohibits the use of any information system for fraudulent or illegal purposes. While using any of the college's information systems, a user must not engage in any activity that is illegal under local, state, federal, and international law. As a part of this policy, users must not:

- Violate the rights of any individual or company involving information protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by the College.
- Use in any way copyrighted material including, but not limited to, photographs, books, or other copyrighted sources, copyrighted music, and any copyrighted software for which the College does not have a legal license.
- Export software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Issue statements about warranty, expressed or implied, unless it is a part of normal job duties, or make fraudulent offers of products, items, and/or services.

Any user that suspects or is aware of the occurrence of any activity described in this section, or any other activity they believe may be fraudulent or illegal, must notify his/her supervisor who must inform the Office of Human Resources, the Chief Information Officer and the Information Security Officer immediately thereafter. Violators will be subject to penalties described in the Enforcement section of this policy.

B. Protection of Confidential Information – The College has both an ethical and legal responsibility for protecting confidential information in accordance with the Data Classification Policy. To that end, these are some general precautions employed by the College:

- Transmission of confidential information by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is prohibited.
- The writing or storage of confidential information on mobile devices (phones, tablets, USB drives) and removable media is prohibited. Mobile devices that access confidential information will be physically secured when not in use and located to minimize the risk of unauthorized access.
- Photographic, video, audio, or other recording equipment will not be utilized in secure areas where confidential information is maintained.

- The use of non-approved workstations or devices to access College's data, systems, or networks by employees and service providers when handling confidential information is prohibited. Non-College owned workstations that store, process, transmit, or access confidential information are prohibited. Accessing, storage, or processing College's restricted or private information on home computers is prohibited.
- All of the College's portable workstations will be securely maintained when in the possession of employees. Such workstations will be handled as carry-on (hand) baggage on public transport. They will be concealed or locked when in private transport (e.g., locked in the trunk of an automobile) when not in use. Employees will activate their workstation locking software whenever they leave their workstation unattended or will log off from or lock their workstation when their shift is complete.
- Employees who use College-owned workstations will take all reasonable precautions to protect the confidentiality, integrity and availability of information contained on the workstation. All confidential information stored on workstations and mobile devices must be encrypted.
- Employees and affiliates who move electronic media or information systems containing confidential information are responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft and unauthorized use.

C. Harassment – The College is committed to providing a safe and productive environment, free from harassment, for all employees. For this reason, users must not:

- Use College's information systems to harass any other person via e-mail, telephone, or any other means, or actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws.
- If a user feels he/she is being harassed through the use of the College's information systems, the user must report it, in writing, to his/her supervisor or any department head.

D. Incident Reporting - Security incidents involving personnel, College-owned information or College-owned information assets must be timely responded to. As part of this policy:

- The loss, theft or inappropriate use of the College's access credentials (e.g. passwords, key cards or security tokens), assets (e.g. laptop, cell phones), or other information must be immediately reported to the Information Technology Services (ITS) Service Desk.
- An employee will not prevent another employee from reporting a security incident.

E. Malicious Activity – The College strictly prohibits the use of information systems for malicious activity against other users, the College's information systems themselves, or the information assets of other parties. Users must not:

- Perpetrate, cause, or in any way enable disruption of the College's information systems or network communications by denial-of-service methods;
- Knowingly introduce malicious programs, such as viruses, worms, and Trojan horses, to any information system; or
- Intentionally develop or use programs to infiltrate a computer, computing system, or network or damage or alter the software components of a computer, computing system or network.

F. User Restrictions - Users must not:

- Perpetrate, cause, or in any way enable security breaches, including, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access;
- Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends;

- Use the same password for the College accounts as for other non- College access (for example, personal ISP account, social media, benefits, E-mail, etc.);
- Attempt to gain access to files and resources to which they have not been granted permission, whether or not such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password;
- Make copies of another user's files without that user's knowledge and consent.
- All encryption keys employed by users must be provided to Information Technology Services (ITS) if requested, in order to perform functions required by this policy.
- Base passwords on something that can be easily guessed or obtained using personal information (e.g. names, favorite sports teams, etc.).
- Circumvent the user authentication or security of any information system;
- Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information;
- Create or use a proxy server of any kind, other than those provided by the College, or otherwise redirect network traffic outside of normal routing with authorization;
- Use any type of technology designed to mask, hide, or modify their identity or activities electronically.
- Use a port scanning tool targeting either the College's network or any other external network, unless this activity is a part of the user's normal job functions, such as a member of the Information Technology Services, conducting a vulnerability scan, and faculty utilizing tools in a controlled environment.
- Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the user unless this activity is a part of the user's normal job functions.
- Stream video, music, or other multimedia content unless this content is required to perform the user's normal business functions;
- Use the College's information systems for commercial use or personal gain or to play games or provide similar entertainment.

G. Objectionable Content - The use of College's information systems for accessing or distributing content that other users may find objectionable is strictly prohibited. Users must not post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials considered to be political, racist, sexually-explicit or promoting violence.

Examples of possible objectionable, improper or inconsistent use of the College's technology resources include:

- Forwarding appeals soliciting donations to individuals or charities;
- Distributing communications that promote religious, political or personal preferences and activities;
- Sending or forwarding messages containing libelous, defamatory, offensive, sexist, racist or obscene remarks;
- Forging or attempting to forge messages, or disguise identity;
- Utilizing a personal E-mail account (i.e. Outlook, Yahoo!, Gmail, Hotmail, etc.) to conduct college-related matters;
- Downloading, using or distributing illegally obtained media (e.g. software, music, movies);
- Uploading, downloading, distributing or possessing pornography.

H. Hardware and Software - The use of any hardware or software that is not purchased, installed, configured, tracked, and managed by the College is prohibited. Users must not:

- Install, attach, connect or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to College's information system without the knowledge and permission of Information Technology Services staff;
- Download, install, disable, remove or uninstall software of any kind, including patches of existing software, to any institutional information system without the knowledge and permission of the College's Chief Information Officer (CIO);
- Use personal flash drives, or other USB based storage media, without prior approval from their manager and the Information Security Officer (ISO)
- Take Old Westbury equipment off-site without prior authorization.

I. Group/Mass E-Mail and other Communications - Mass communications should be used sparingly. Many academic and administrative entities on campus are interested in using Email and other digital communication services, such as text messaging, to send important *but unsolicited messages* to large segments of the college community: for example, to all students, all faculty, all staff, or to some combination of these large segments. To moderate the use of sending college-wide digital messages, the College will periodically employ its Alert Notification System to reach the majority of the college community. Presently the Alert Notification System is on an "opt-in" basis which may be subject to a policy change.

If a faculty member, staff or student desires to send an E-mail message to multiple parties at the same time for group announcements or news, an E-mail distribution list can be created within the Alert Notification System.

- Distribution lists and groups within the E-mail system will be moderated and monitored by the Information Security Officer (ISO) for proper usage; and
- If a distribution list or group becomes inactive for a period of six months, it will be removed from the college E-mail system.

Mass digital communications can also be utilized when a college emergency or an urgent need-to-know matter warrants their use. If a college-wide digital message is deemed appropriate and time-critical by the Office of the President, University Police, or the Office of Communications, the message should be sent to the College's Chief Communications Officer for distribution to the intended parties. Appropriate content topics include, but are not limited to: (1) urgent security (physical and electronic) matters; (2) natural disaster alerts; (3) significant campus-wide policy changes; and (4) time-critical administrative announcements.

J. Messaging – The College provides a robust communication platform for users. However, Users must not:

- Automatically forward electronic messages of any kind, by using client message handling rules or any other mechanism;
- Send unsolicited electronic messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (spam);
- Solicit electronic messages for any other digital identifier (e.g., e-mail address, social handle, etc.), other than that of the poster's account, with the intent to harass or to collect replies; or
- Create or forward chain letters or messages, including those that promote "pyramid" schemes of any type.

K. Remote Work - When working from a remote site, user must:

- Safeguard and protect any institution-owned or managed computing asset (e.g. laptops and cell phones) to prevent loss or theft.
- Not utilize personally-owned computing devices for work, including transferring College's information to personally-owned devices, unless approved by Information Security Officer.

- Take reasonable precautions to prevent unauthorized parties from utilizing computing assets or viewing information processed, stored or transmitted on College-owned assets.
- Not create or store confidential or official information on local machines unless a current backup copy is available elsewhere.
- Not access or process confidential information in public places or over public, insecure networks.
- Only use approved methods for connecting to the college's technical resources (e.g. VPN).

VI. PRIVACY

The College will make every reasonable effort to respect a user's privacy. However, employees do not acquire a right of privacy for communications transmitted or stored on the College's resources. Additionally, in response to a judicial order or any other action required by law or permitted by official SUNY Old Westbury policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the College's Chief Information Officer, in consultation with the Senior Vice President of Business & Finance and the Assistant to the President for Administration, may authorize an Old Westbury official or an authorized agent, to access, review, monitor or disclose computer files associated with an individual's account. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or the College's rules, regulations or policy, or when access is considered necessary to conduct the College's business due to the unexpected absence of an employee or to respond to health or safety emergencies.

The College reserves the right to protect, repair, and maintain its computing equipment and network integrity. In accomplishing this goal, the College's ITS (Information Technology Services) personnel or their agents must do their utmost to maintain user privacy, including the content of personal files and Internet activities. Any information obtained by ITS personnel about a user through routine maintenance of the College's computing equipment or network should remain confidential, unless the information pertains to activities that are not compliant with this policy.

VII. ENFORCEMENT AND EXCEPTIONS

Enforcement is the responsibility of SUNY Old Westbury's President or designee. Users who violate this policy may be denied access to the institutional resources and may be subject to penalties and progressive disciplinary action up to possible expulsion or dismissal. The College may temporarily suspend or block access to an account prior to the initiation or completion of disciplinary procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the College's computing resources or to protect the College from liability. If any user creates a liability on behalf of the College due to inappropriate use of the College's digital information assets, the user agrees to indemnify and hold the institution harmless, should it be necessary for the College to defend itself against the activities or actions of the user.

Alleged violations will be handled through the College's disciplinary procedures applicable to the user, and other policies and procedures governing acceptable workplace behavior. When the Information Technology Services (ITS) Department becomes aware of a possible violation, an investigation will be initiated in conjunction with the College's Information Security Officer (ISO) and relevant campus officers. Users are expected to cooperate fully in such investigations when requested. If warranted, the College may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Exceptions to the policy may be granted by the Chief Information Officer or designee, in consultation with the Senior Vice President of Business & Finance. All exceptions must be reviewed annually.

VIII. REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- New York State Information Security Breach and Notification Act
- National Institute of Standards and Technology (NIST) 800-53
- Federal Information Processing Standard (FIPS) -199
- Payment Card Industry Data Security Standard (PCI DSS) 3.1
- New York Civil Practice Law and Rules § 4509 Photographic, video, audio, or other recording equipment will not be utilized in secure areas where confidential information is maintained.
- Code of Ethics of the American Library Association

IX. APPROVALS

This policy was prepared by the Division of Business & Finance in consultation with the Senior Vice President of Business & Finance, the Chief Information Officer, the Information Security Officer, the Vice President of Communications and the Assistant to the President for Administration prior to approval by the President.

This policy supersedes previously issued College Policies: B-03 “E-mail Procedures” (August 2014), C-01 “Internet Security Policy” (October 2002) and C-05” Acceptable Use of College Technology Resources” (September 2013).