I. POLICY

SUNY Old Westbury (College) established this Information Security Policy to: assist College personnel in fulfilling responsibilities relating to the protection of information assets; and, to comply with statutory and contractual requirements involving information security and privacy. The Policy acts as an umbrella document to all information security policies, associated standards and controls.

II. PURPOSE and SCOPE

The purpose of this Policy is to clearly delineate the College's role in protecting its information assets and to communicate the minimum expectations for meeting these requirements. Fulfilling these objectives enables the College to implement a comprehensive system-wide *Information Security Program* **(ISP)**.

The scope of this policy encompasses all systems, automated and manual, for which the College has administrative responsibility, including systems managed or hosted by third parties on behalf of the College. All personnel and service providers who have access to or utilize the information assets of the College, including data at rest, in transit or in process shall be subject to these requirements.

III. RESPONSIBILITIES

The College needs to protect the confidentiality, integrity and availability of data while providing information resources to fulfill its mission. This will be achieved via the **ISP**. The College Administration recognizes that fully implementing all controls within the National Institute of Standards and Technology (NIST) framework is not possible due to institutional limitations and resource constraints. The College Administration, however, must implement NIST standards whenever possible and document exceptions where doing so is not practicable.

The College's *Chief Information Officer (CIO*) is accountable for the implementation and monitoring of the **ISP** including, security policies, standards procedures and the related managerial, administrative and technical controls. The College's *Information Technology Services (ITS) department*, under the direction of the CIO, will also work with SUNY and vendors to arrange the requisite security training for employees.

The College's *Information Security Officer (ISO)* is responsible for the development and maintenance of a comprehensive **ISP** for the College. This includes information security policies, standards and procedures which reflect best practices in information security. The ISO is also responsible for reviewing and periodically updating this Policy.

IV. DEFINITIONS

A. *Information Asset* is any application, system or solution used by the College that creates, receives, maintains or transmits restricted or private data, such as protected health information, personally identifiable information, payment card data, or financial data, etc.
B. *Authorized User* is any individual granted credentials to access the College's information assets.
C. *Credentials* refer to the unique username and password provided each authorized user to access the College's information assets.
D. *Digital Information* is the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing manually or electronically.
E. *Security Boundaries* are a set of information systems that are under a single administrative control.

V. PROCEDURES

The College's **ISP** is framed on NIST standards and controls implemented based on SysAdmin, Audit, Network and Security (SANS) Critical Security Controls priorities. The College must develop appropriate control standards and procedures required to support this policy which is further defined by control standards, procedures, control metrics and control tests to assure functional verification. The **ISP** is structured into 18 security domains designed to meet all statutory and contractual requirements. Accordingly, the College must implement standards and controls that address:

(1) ACCESS CONTROL - Limit its information system access to authorized users, processes acting on behalf of authorized users or devices and to the types of transactions and functions that authorized users are permitted to perform.

(2) AWARENESS AND TRAINING - Ensure that all users of its information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of the systems; and ensure that the College employees are adequately trained to carry out their assigned information security-related duties and responsibilities.

(3) AUDIT AND ACCOUNTABILITY - Create, protect, and retain system audit records to the extent required to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

(4) ASSESSMENT AND AUTHORIZATION - Periodically assess the security controls to determine their effectiveness; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities; authorize the operation of the information systems and monitor the security controls on an ongoing basis to ensure the continued effectiveness of the controls.

(5) CONFIGURATION MANAGEMENT - Establish and maintain baseline configurations and inventories of its information systems (including hardware, software, firmware, and documentation) as well as enforce established security configuration settings.

(6) CONTINGENCY PLANNING - Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for its information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

(7) IDENTIFICATION AND AUTHENTICATION - Identify information system users, processes acting on behalf of users, or devices, and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to the information systems.

(8) INCIDENT RESPONSE -Establish operational incident handling capability for its information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, along with the ability to track, document, and report incidents to appropriate College officials or authorities.

(9) MAINTENANCE - Perform periodic and timely maintenance on institution information systems; and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

(10) MEDIA PROTECTION - Protect information system media, both paper and digital; limit access to authorized users; and apply encryption, where applicable, sanitize or destroy information system media before disposal or release for reuse.

(11) PHYSICAL AND ENVIRONMENTAL PROTECTION - Limit physical access to its information systems, equipment and the respective operating environments to authorized employees; secure the physical location and supporting infrastructure while providing necessary utilities and environmental controls to protect against environmental hazard.

(12) PLANNING - Develop, document, periodically update and implement security plans that describe the security controls in place or planned as well as rules of behavior for individuals accessing the College's information systems.

(13) PERSONNEL SECURITY - Ensure that individuals occupying positions of responsibility within the institution meet established security criteria for those positions; ensure that information assets are protected during and after events such as terminations and transfers; and employ formal sanctions for employees failing to comply with the College's information security policies and procedures.

(14) RISK ASSESSMENT - Periodically assess the risk to its operations (including mission, functions, image, or reputation), institutional assets, and individuals, resulting from its information assets and the associated processing, storage or transmission activities.

(15) SYSTEM AND SERVICES ACQUISITION - Allocate sufficient resources to adequately protect information systems; employ system development life cycle processes that incorporate information security considerations; employ software usage and installation restrictions; and ensure that third- party providers employ adequate security measures, through federal and state law and contract, to protect information, applications or services outsourced from the College.

(16) SYSTEM AND COMMUNICATIONS PROTECTION - Monitor, control and protect communications (i.e., information transmitted or received by the College's information systems) at all security boundaries for confidential data transmissions; and employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within its information systems.

(17) SYSTEM AND INFORMATION INTEGRITY - Identify, report and correct information and information system flaws in a timely manner; provide protection from malicious code and monitor information system security alerts and advisories to take appropriate actions in response.

(18) PROGRAM MANAGEMENT - Implement security program management controls to provide a foundation for its **ISP**.

VI. ENFORCEMENT AND EXCEPTIONS

Enforcement is the responsibility of SUNY Old Westbury's President or designee. The CIO, in consultation with the President or the President's designee, may prevent, based on security or legitimate business concerns in whole or in part, any user from accessing institutional data at any time, without notice.

The College may also temporarily suspend or block access to an account prior to the initiation or completion of disciplinary procedures, when it reasonably appears necessary to protect the integrity, security, or functionality of the College's computing resources or to protect the College from liability. Violators of this Policy will be subject to the College's disciplinary procedures and depending on the nature and severity of the violation. Severe violations may be referred to appropriate law enforcement agencies.

Exceptions to this Policy may be granted by the CIO, in consultation with the President or the President's designee. All exceptions must be reviewed annually.

VII. REFERENCES

- National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53)
- Family Educational Rights and Privacy Act (FERPA)
- The Gramm - Leach Bliley Act (GLBA)
- SUNY Old Westbury's Data Classification Policy (C-08)
- New York State Information Security Breach and Notification Act
- Federal Information Processing Standard Publication 199 (FIPS-199)
- Payment Card Industry Data Security Standard version 3.1 (PCI-DSS 3.1)

VIII. APPROVALS

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