I. POLICY

It is the policy of SUNY Old Westbury (College) to provide guidance regarding the appropriate classification of its data. This Data Classification Policy is designed to maintain high standards regarding information security by protecting the College's digital information assets.

II. PURPOSE and SCOPE

The purpose of this Policy is to define the data classification requirements for digital information assets and to ensure that institutional data is secured and handled according to its sensitivity. This policy provides directions regarding identification, classification and handling of digital information assets. Further, compliance with this policy will mitigate any impact that theft, corruption, loss or exposure would have on the College.

This policy includes all digital information assets governed by the College. All personnel and third parties who have access to or utilize digital information assets to process, store and/or transmit information for or on the behalf of the College shall be subject to these requirements.

III. RESPONSIBILITIES

Data owners are accountable for ensuring that their digital information assets receive an initial classification upon creation and a re-classification whenever reasonable. Re-classification of an information asset should be performed by the asset owners whenever the asset is significantly modified. Additionally, data owners are responsible for reporting deficiencies in security controls to management.

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 non-public institutional data at any time, without notice.

The College's *Information Security Officer (ISO)* is responsible for overseeing and coordinating the implementation of College policies governing information security and privacy on Internet. The ISO is responsible for reviewing and updating (if necessary) the Data Classification Policy annually.

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

A **Data Owner** is an individual or committee primarily responsible and accountable for specific digital information assets (data). Data ownership is the concept wherein a person/position or group owes the rights to control access to a particular set or group of data. Data ownership refers to the rights of the creator of data as opposed to the subject of the data which can be used by other College personnel. For example, the Office of the Registrar is the owner of student registration data even though the Office of Institutional Research has access to the data and uses in preparing College reports. Other examples of data owners include the Division of Business & Finance for financial data and the Office of Human Resources for employee data.

Data Owners are responsible for:

- Identifying the institution's digital information assets under their areas of supervision; and
- Maintaining an accurate and complete inventory for data classification and handling purposes.

Employee Directory Information is defined as the following:

- Name; Date of hire; Date of separation; Current position title; Employment status; Department of assignment, including office telephone number and office address.

V. PROCEDURES

A. **Data Handling –** Digital Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods. The specific methods must be described in the Data Classification Procedure.

B. **Classification Inheritance -** Logical (Virtual Desktop) or physical assets (computers, laptops, tablets, etc.) that "contain" a digital information asset may inherit classification from the data contained therein. In these cases, the inherited classification shall be the highest classification of all contained digital information assets.

C. **Re-Classification -** A re-evaluation of classified digital information assets will be performed at least once per year by the responsible data owners. Re-classification of data assets should be considered whenever the data asset is modified, retired or destroyed.

D. **Data-Classification -** Classification of data will be performed by the digital information asset owner based on the specific, finite criteria. The Data Classification Schema does not limit nor restrict data access to research data by its author or designee; it does not impinge on academic freedom or the rights of researchers to control their own data/findings. Rather, the Data Classification Schema provides criteria for the loss of said data, its impact on the College and the level of protection required.

Data classifications will be defined as follows:

- **RESTRICTED** - Information whose loss, corruption, or unauthorized disclosure would cause severe personal, financial or reputational harm to the college, to employees or to the constituents that the college serves. Federal or state breach notification would be required, identity or financial fraud, extreme revenue loss, or the unavailability of extremely critical systems or services would occur. Common examples include, but are not limited to, some elements of Family Educational Rights and Privacy Act (FERPA) data, social security number (SSN), banking and health information, Payment Card Information (PCI) and information systems' authentication data.

  The Breach Notification Act applicable to **RESTRICTED** data requires the College to disclose any breach of the data to NYS residents. (State entities must also notify non-residents). See New York's Information Security Policies at https://www.its.ny.gov/eiso/policies/security.

- **PRIVATE** - Information whose loss, corruption, or unauthorized disclosure would cause limited personal, financial or reputational harm to the college, to employees or to the constituents that the college serves. Federal or state breach notification would not be required, limited identity theft and very little revenue loss would occur, and the availability of critical systems would not be affected. Common examples include, but are not limited to, some elements of Family Educational Rights and Privacy Act (FERPA) data, some data elements found in Student Information System (SIS) records, unpublished research data, passport and visa numbers, public safety information, the College's infrastructure data, collective bargaining/contract negotiation data, college intellectual property, college proprietary data, data protected by non-disclosure agreements,

college financial data, employee directory information, meeting minutes, administrative process data, licensed software, etc.

- **PUBLIC** - Information whose loss, corruption, or unauthorized disclosure would cause minimal or no personal, financial or reputational harm to the College, to employees or to the constituents that the college serves. Federal or state breach notification would not be required. Common examples include, but are not limited sales and marketing strategies, promotional information, published research data, and policies.

VI. 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 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 Old Westbury 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 Old Westbury 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.

Where data security concerns are significant, employee access to the data may be limited or removed. 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.

VII. REFERENCES

- Federal Information Processing Standard Publication 199 (FIPS-199)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- SUNY Old Westbury's Acceptable Use of College Technology Resources Policy (C-05)
- New York State Information Security Breach and Notification Act
- National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53)

VIII. 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, and the Information Security Officer. It was reviewed by the President's Cabinet prior to approval by the President.