I. POLICY:

This policy defines standards, procedures, and restrictions for physical access to SUNY Old Westbury's Network Data Closets and the Data Center. It is designed to protect the College's information technology-based resources (such as institutional data, computer systems, networks or other network devices) from unauthorized use or malicious attacks that could result in loss of information, damage to critical applications, loss of revenue, and damage to the College' public image.

II. PURPOSE and SCOPE:

The overriding goal of this policy is to reduce informational and operating risks. Adherence to this policy and related procedures will:

- Regulate unauthorized traffic in a secure facility to minimize exposure to data breach risks and activities that cause network and various systems related outages.
- Facilitate compliance with the SUNY Information Security Policy and technology standards for Higher Educational Institutions which require universities to implement IT controls and demonstrate the controls are working.
- Protect institutional Data, the Data Center and Network Data Closets from unauthorized use or a malicious attack.

III. RESPONSIBILITIES:

Access to Network Data Closets and the Data Center owned or operated by the College must be controlled, monitored and audited in a manner that adheres to the defined processes established by the College.

The College's Chief Information Officer (CIO) has the overall responsibility for implementing this policy and for the confidentiality, integrity, and availability of institutional electronic data. The Information Technology Services (ITS) staff under the direction of the CIO, is responsible for monitoring compliance with this policy and related procedures.

The designation or creation of new network or server rooms within the College will be managed by ITS in consultation with the Facilities Department.

IV. PROCEDURES:

A. Employee Access

The Data Center is physically secured by a card-reader door lock and monitored 24 hours a day/ 7 days a week by University Police Department (UPD). Recorded video surveillance is conducted through the security cameras placed within and outside of the Data Center. Card-reader access is available to the Data Center on a 24 hours a day/7 days a week basis for authorized employees.

1. Enterprise Infrastructure Services (EIS), University Police Department and the Heat Plant (Facilities) staff have been authorized for access based on job related needs. The need for authorization will be reviewed annually by the College's Information Security Officer (ISO) or the CIO.
2. Staff must wear their identification badge at all times.
3. Entry into the Data Center or Network Data Closets by 'tailgating' other staff is strictly forbidden.
4. EIS staff must report all security or health and safety incidents regarding the Data Center or Network Data Closets to the ISO or the CIO immediately.

5. Two sets of physical keys exist to override the card-reader and open the doors in the event of a failure. These sets of keys are stamped 'Do Not Duplicate'.
6. EIS staff will accompany visitors in Data Center or Network Data Closets at all times.
7. EIS staff is expected to challenge any unescorted visitors within the Data Center or Network Data Closets.

B. Vendor Access

The following procedures apply to vendors seeking access to the Data Center or Network Data Closets.

1. Vendors included in the Approved Vendor Access List have been authorized for access based on job related need. The Approved Vendor Access List is maintained by the ISO and will be reviewed by the ISO or the CIO quarterly.
2. Vendors must wear their identification badge at all times when onsite.
3. Vendors with approved access to the Data Center or Network Data Closets are required to identify themselves to the ISO or the CIO and sign in/out of the Data Center using the Data Center Access Log.
4. Vendor entry into the Data Center or Network Data Closets by 'tailgating' others is strictly forbidden.
5. Vendors are expected to report all security or health and safety incidents regarding the Data Center or Network Data Closets to the ISO or the CIO immediately.

C. Visitor Access

In general, casual visits or tours of the Data Center or Network Data Closets are not allowed. However, approval of a tour or casual visit may be granted. Requests for a visit or tour of these secured facilities should be directed to the CIO or the ISO.

1. Visitors are required to identify themselves to the ISO or the CIO and sign in/out of the server room using the Site Access Log.
2. Visitors must be escorted at all times while onsite.
3. Visitors will be made aware of this policy. It is the responsibility of the staff member accompanying the visitor to ensure the visitor's conduct conforms to this policy.

D. Data Center or Network Data Closets Access

To maintain a safe and secure environment, it is mandatory for all persons working within and visiting the Data Center or Network Data Closet to adhere to the following rules:

1. Cameras are not permitted and taking photographs is strictly forbidden.
2. The use of mobile phones, pagers or other equipment that emit radio waves within the server room is forbidden unless approved by ISO or the CIO.
3. No food or drink is allowed within the Data Center or Network Data Closets.
4. No Hazardous materials are allowed within the Data Center or Network Data Closets.
5. No cleaning supplies are allowed within the Data Center or Network Data Closets without prior approval.

6. No cutting, grinding, or whittling of any material (pipes, floor tiles, etc.) can be performed inside the Data Center or Network Data Closets unless special arrangements have been made.
7. Only authorized staff shall access the sub-floor or remove floor tile.
8. All packing material (cardboard, paper, plastic, wood, styrene, etc.) must be removed from equipment in the staging area before being moved into the Data Center or Network Data Closets.
9. Staff and visitors must wear identification badge at all times.
10. All persons are expected to report all security or health and safety incidents regarding the Data Center or Network Data Closets to the ISO or the CIO immediately.
11. No person shall connect any equipment, network, wireless devices, or monitoring tools without permission or written authorization of the ISO or the CIO.

E. Monitoring and Audit

Data Center and Network Data closet access is controlled and monitored by various sub-systems (reader door lock system, video surveillance cameras, etc.) which produce access records. All Data Center and Network Data closet access records are subject to the following rules:

1. Access records will be monitored by the EIS Manager, ISO or the CIO. Unauthorized access and access which is inconsistent with staff schedules will be investigated and appropriate action will be taken.
2. Access records produced by the reader door lock system will be maintained and reviewed by University Police Department.
3. Video records will be maintained and reviewed by University Police Department.
4. The Approved Vendor List and the Data Center Closet Access List are maintained and periodically reviewed by the ISO.
5. The Senior Vice President & Chief Financial Officer (CFO), the CIO, and the immediate Manager or Director will be advised by the ISO of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.
6. Any exception to the policy must be approved by the ITS Department in advance.

V. REFERENCES:

1. SUNY Information Security Policy Document 6900
2. National Institute of Standards and Technology NIST 800-171
3. Old Westbury Policy No. C-05 – Acceptable Use of College Technology Resources

VI. APPROVALS:

This policy was prepared by the Division of Business & Finance and reviewed by senior administrators in the Information Technology Services, Facilities and University Police departments prior to approval by the President.