INTRODUCTION:

In order for SUNY Cortland to execute its mission of supporting technology used for teaching and learning, the campus is committed to providing a secure yet open network that protects the integrity and confidentiality of information while maintaining its ease of access.

POLICY:

Each member of the campus community is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to off-campus entities must comply with the same security requirements as in-house activities.

Providers (individuals who design, manage, and operate campus electronic information resources, e.g. application programmers, systems operators, network and system administrators) must:

- become knowledgeable regarding relevant security requirements and guidelines;
- analyze potential threats and the feasibility of various security measures in order to provide recommendations to the administration;
- implement security measures that mitigate threats, consistent with the level of acceptable risk established by administrative officials;
- establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access guidelines;

Users (individuals who access and use campus electronic information resources) must:

- become knowledgeable about relevant security requirements and guidelines;
- protect the resources under their control, such as access passwords, computers, and data they download

Insufficient security measures at any level may cause resources to be damaged, compromised, stolen, or become a liability to the campus. Therefore, responsive actions may be taken. For example, if a situation is deemed serious enough, computer(s) posing a threat will be blocked from network access.

NETWORK TOPOLOGY:

The SUNY Cortland campus network is a converged IP voice/video/data layer 3 network using gigabit Ethernet as the backbone, scalable to 10 gigabit.

KEY SECURITY ELEMENTS:

Logical Security:

All computers connected to the campus network must have the most recently available and appropriate software security patches and the most current level of antivirus installed.

Adequate authentication and authorization functions must be provided.

Attention must be given not only to large systems but also to smaller computers which, if compromised, could constitute a threat to campus or off-campus resources, including computers maintained by departments other than Administrative Computing Services. These computers must follow all campus standard security strategies. **Physical Security:**

Appropriate controls must be employed to protect physical access to all technology resources. These may range in scope and complexity from extensive security installations to protect a room or facility where server machines are located, to simple measures taken to protect a User's display screen.

Minimum Security Standards for SUNY Cortland's Campus Networked Devices

The following minimum standards are required for devices connected to the campus network.

1. Software patch updates

Campus networked devices will be automatically configured to receive the most current security patches as they become available. Exceptions may be made for patches that compromise the usability of critical applications.

2. Anti-virus software

The campus standard Anti-virus software must be running and definitions up-to-date on every level of device, including clients, file servers, mail servers, database servers and any other types of campus networked devices.

3. Enterprise and client levels hardware/software firewall

The campus network will be segmented and protected at all times from potential intrusion by an enterprise level firewall hardware device.

Host-based firewall software for any particular type of device currently connected to the campus network must be running the campus standard host-based firewall software.

4. Passwords

All departmental and shared access clients (desktops, handhelds, and tablet PC's) and servers connected to the campus network must identify users and authorize access by means of passwords or other campus standard secure authentication processes.

All default passwords for access to network-accessible devices must be modified.

Passwords:

- will have a maximum lifetime of 6 months
- must be at least 6 character in length
- will have password history enforced
- will auto expire at initial login
    i. Note: students assign their own password so this will not relate to them

Passwords used by system administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device.

5. No unencrypted authentication

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the campus network may be secretly monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all campus devices must use only encrypted authentication mechanisms unless otherwise authorized.

6. No unauthenticated email relays

Campus devices must not provide an active SMTP service that allows unauthorized third parties to relay email messages, i.e., to process an e-mail message where neither the sender nor the recipient is a local user. Before transmitting email to a non-local address, the sender must authenticate with the SMTP service. Authenticating the machine (e.g. IP address/domain name) rather than the sender is not sufficient to meet this standard.

7. Remote Access

Off campus access to all campus technology resources will be provided through a Virtual Private Network (VPN) hardware appliance. Off campus client machines will be required to run the campus standard VPN software to gain access to campus technology resources.

8. No unauthenticated proxy services

Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Therefore, no unauthenticated proxy servers will be allowed to run on the campus network.

9. Physical security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for a predetermined period of time.

Physical security of the campus server room is a critical component of information security and should not be taken lightly. Physical access to the campus server room must be granted and authorization given by the campus CSO (Cyber Security Officer). The CSO will request from the campus card access administrator to grant access to the server room for a specific day and period of time. At the end of which access will again be denied to all unauthorized individuals.

Entities with important campus electronic information security responsibilities include:

CIO – Chief Information Officer
CSO - Chief Security Officer