Section 1: Introduction
City College Network Management Policies and Procedures provide the operational detail required for the successful implementation of a safe and efficient computer network environment. These security regulations were developed based on the educational and administrative needs of the College and an evaluation of the existing technical configuration and requirements.

Section 2: Network Node Policies
2.1 Administrative Computer Authentication System
The City College Information Technology Services department (ITS) will maintain a centralized computer authentication system for Administrative computers (Faculty and Staff) using Microsoft Active Directory (AD) services. All college-owned networked computers which are capable of utilizing this authentication system will be configured to verify login credentials with AD.

2.2 Standard Configuration
All City College owned networked computers will have a standardized image developed and tested by the Desktop Services Department. These settings will provide a minimum baseline configuration that will ensure computer network security and integrity. All Windows computers will be equipped with anti-virus software. All reasonable measures will be taken to keep pirated software from being installed on any CCSF computer.

2.3 Naming Convention
All City College owned computers and printers will use a standard naming convention.

2.4 Administrative Access
Network Services will have administrative level access to all college-owned computers which are connected to the computer data network reserved for Faculty and Staff.

2.5 IP Address Assignments
City College Administrative computers (Faculty and Staff) will generally use Dynamic IP Addressing (DHCP) for IP address assignment. The VLAN assignment for a given computer will be made by Desktop Services or Network Services as appropriate.

2.6 Authorized Servers and Services
Network Services will have access to a list of all computers connected to the computer data network which are running any network service remotely accessible by another computer. The list will be maintained by the Technical Operations Group. Only computers which appear in this list are allowed to run the network services for which they are authorized. If a previously approved network service on a computer has been found to cause network degradation, violate College policies, or violate local, state, or federal laws, the owner of the respective service will be notified for resolution of the issue. If the the network service or the host server is found to be
affecting critical District-wide systems such as Banner or Groupwise it will be temporarily removed from the network and the owner of the respective service will be notified.

2.7 Web Accessible Information
Web Servers not maintained by ITS will have a designated individual who will be responsible for maintaining the associated server as follows:
- The operating system and applications must be regularly updated and patched.
- An actively running virus scanner must be used with the latest virus definitions.

2.8 Privately Owned Computers
Computers that are connected to the computer data network reserved for Faculty and Staff, but not owned by the College should be configured to ensure reasonable network security and integrity. The computer must be configured but not limited to the following:
- The operating system and applications must be updated and patched.
- An actively running virus scanner must be used with the latest virus definitions.
Privately-owned computers which are found to be performing activities which cause network degradation, violate College policies, or violate local, state, or federal laws, will not be allowed to connect to the computer data network reserved for Faculty and Staff.

2.9 Account Login Information Sharing Prohibited
Accounts are to be used only by the persons to whom the accounts are assigned. Log-on IDs, passwords, and other means of access are not allowed to be shared with any other individual.

2.10 Classroom Access
All CCSF classrooms will be provided with an active wired data jack for Internet access. Access will not require authentication and will accommodate all makes of computers capable of utilizing Dynamic IP Addressing (DHCP). These wired jacks are only for use by faculty and staff.

2.11 Regulatory Adherence
It is the responsibility of Faculty, Staff and Students to adhere to all local, state or federal regulations governing network operations initiated while this policy is in effect.

Section 3: Network Infrastructure Policies
3.1 Firewall/VLAN Configuration
The City College firewall and/or VLANs will provide a separation of the Administrative (Faculty and Staff) network and the Instructional (Student) network in order to reduce the potential for unauthorized access of confidential data and other technology-based resources.

3.2 Firewall Changes
Requests for Network Services which require a firewall configuration change will be evaluated by the Network Services Department as part of the ITS project evaluation process. Requested changes which could jeopardize the security and integrity of the City College data network will not be implemented.

3.3 Peer-to-Peer Traffic
It is a violation of the Higher Education Act to allow peer-to-peer file sharing of copyrighted material. An application-aware firewall will be maintained by the Technical Operations Group in ITS, in order to meet this requirement. In accordance with the Higher Education Act all Faculty,
Staff and Students will be provided with an annual disclosure that explicitly informs them that the unauthorized distribution of copyrighted material may subject them to civil and criminal liabilities.

3.4 URL/IP Filtering
There will be no URL-based blocking other than as required by law. Access to and from IP addresses that are determined to be a security threat will be restricted in order to protect against malware, worms, viruses, Trojans and other types of malicious activities. These restrictions will have a time limit, and will be specified to individual IP addresses, not ranges of addresses. When IP addresses are blocked, the reason for such blockage will be documented. The guiding principle of academic freedom shall be applied when ITPC reviews the criteria that are used to maintain any list of blocked URLs and/or IPs, which might be blocked for either incoming or outgoing traffic. The ITS department shall document and report on a regular basis to the ITPC the decisions it has made to implement this section.

3.5 Secure Systems Access
All CCSF systems requiring web-based authentication will utilize Hypertext Transfer Protocol Secure (https) or other encrypted protocols for encryption and security identification.

3.6 WiFi Radios
Network access using WiFi technology will be provided for City College Faculty, Staff and Students utilizing WPA2 encryption. Access for Guests will be provided in limited areas and will be unsecured. Additional WiFi access points can be utilized for specialized purposes based on approval from Network Services. WiFi access points attached to the Administrative network are not authorized and will be disconnected when discovered.

3.7 Ethernet Switches
All managed switches will use the SSH2 protocol for remote access. Unmanaged switches and hubs approved by the Network Services Department will be authorized in situations that require additional data outlets beyond the number currently available.

3.8 Remote Network Access
A secure Virtual Private Network (VPN) will be maintained to provide access to network-attached resources from outside City College. Authorized employee VPN services include Banner access and IT support. Vendors and contractors may be provided access for technical support of specific services as required.

3.9 Service Providers
All agreements and contracts with communications service providers for telephone, Internet and cellular services will be coordinated by the Network Services Department.

Section 4: Regulation Revision Process
4.1 Changing Environment
The educational, administrative, technical, regulation, and legal environment of City College, as it relates to information technology use and security, is constantly changing. The Network Management Policies and Procedures will be revised as needed to comply with changes in law or administrative rules or to enhance its effectiveness.
4.2 Change Process
Updates to the Network Management Policies and Procedures, which includes creating new policies, modifying existing policies, or removing policies, can result from two different processes:
- At least annually, the Manager of Technical Operations or designate, will review the Policies for possible addition, revision, or deletion.
- New computer network technology introduced into the College will require a documented security assessment by the ITS Management Team. The result of the security assessment could necessitate changes to the Network Management Policies and Procedures before the technology is placed into use.
- Updates to the Network Management Policies and Procedures must be approved by ITPC.

4.3 Change Distribution and Notification
Once a change to the Network Management Policies and Procedures has been made, the following steps will be taken as appropriate to properly document and communicate the change:
- The appropriate Network Security web pages will be updated with the change
- Training and compliance materials will be updated to reflect the change
- The changes will be communicated using standard City College communications methods such as email, announcements, web pages, and newsletters, as necessary.

4.4 Exception Process
The steps for permitting and documenting an exception are:
- A request for an exception is received by the Manager of Technical Operations or designate along with a rationale for justifying the exception.
- The ITS Management Team analyzes the request and the rationale and makes a recommendation to the Information Technology Policy Committee (ITPC) regarding whether the exception should be accepted or denied, or alternative options pursued. ITPC ultimately approves or denies all requests.

4.5 Disputes and Appeals
Disputes regarding this regulation should be sent to the attention of the Manager of Technical Operations.

Appeals to any decision arising from this document should be sent to the Chief Information Technology Officer, then to the ITPC if necessary.