# Chabot Las Positas Community College District
## Networking Standards and Policy

Effective date: TBD

**Wireless and Public Access Network Connection Standards, Policy and Procedures**

### I. Scope and purpose

The purpose of this document is to provide standards, policies, and procedures for the installation, operation, and security of wireless network hardware and public access wired network connections.

### II. Definitions

A. Wireless Network Hardware: Any equipment designed to provide access to the CLPCCD data network through a wireless pathway for any purpose.

B. Public access wired network connection: Any hardwired connection that is intended to provide connectivity to the CLPCCD data network, that is in an area which is largely unsupervised, and/or is intended to provide public access using a privately owned computer.

C. Domain: Any sub-net or group of sub-nets that are created to operate in the two major network domains maintained by the CLPCCD, Administrative, and Faculty/Instructional.

### III. Policy

A. CLPCCD recognizes that there will situations that require other than traditional hard-wired network connections to its data network. These situations may include, but are not limited to:

1. Lack of adequate cable raceways,
2. Cost effectiveness,
3. Portability,
4. Remote device management,
5. Student access and research.

B. Additionally wired connections that are largely unsupervised, may need to be provided for public access to the CLPCCD data network. These would include, but are not limited to:

1. Learning Resource Centers,

2. Student Centers,

3. Information Kiosks,

4. Remote Instructional Areas.

C. Prior to any wireless access hardware being purchased, installed, or placed in operation or any wired access point being activated that is designated for public access, the procedure outlined in paragraph IV below will be followed without exception.

D. Only wireless hardware that complies with the standards set forth in paragraph V below will be purchased, connected and placed into operation on the CLPCCD data network.

**IV. Procedures:**

A. Authorization: Request for the use of a Wireless Access Point or activation of a public access wired connection will be submitted in writing to the Dean of Technology at the respective college for coordination with the District Chief Technical Officer or their designated representative. The request will include the following information as a minimum:

1. The make, model, and technical specifications of the equipment,

2. The area and time period(s) of the working day it is required to be operation,

3. The purpose for which it will be used (how many computers, printers or other peripheral devise will be networked etc.),

4. Justification for its use,

5. What sites and devices will need to be accessed over the network.

B. Security

Recognizing the different levels of security, from network access to student

1. Wireless access points and public access wired connections should be assigned to a special sub-net (when possible) designed for that purpose.

2. When possible, wireless connections will be connected to a managed network switch port. A managed port will enable Cisco Works to automatically disable network access during non- working hours.

3. When not in use wireless access points will be turned off.

The four wireless service classes are indicated in the matrix below:

| **Classes –>** | **OPEN** | **INSTRUCTIONAL** | **ADMIN** | **RESTRICTED** |
|---|---|---|---|---|
| **Open Subnets** | **X** | | | |
| **Instructional Subnets** | | **X** | | |
| **Admin Subnets** | | | **X** | |
| **Special Subnets** | | | | **X** |
| **Security Steps** – > | | | | |
| **Disable Switch Port** | **X** | **Desired /not required** | | |
| **DMZ** | **X** | | | **X** |
| **WEP Security** | | | **X** | **X** |
| **MAC Filtering** | | | **X** | **X** |
| **SSID Turned Off** | | **X** | **X** | **X** |
| **VPN** | | | | **X** |

**OPEN**: This class is designed primarily for use by devices not owned or controlled by CLPCCD. Usage is limited to the Internet, during normal hours of operation. The access point's network port should be disabled during hours of non-operation.

**INSTRUCTIONAL**: This class is for instructional purposes and may connect to other instructional and faculty subnets. Access points should be setup so that they will not broadcast their SSID's and should be disconnected when not in use. Other restrictions may be added as required.

**ADMIN**: This class is for use on the administrative subnets and is the most restrictive. SSID broadcasts will be disabled, MAC filtering, and WEP Security should be used. As new security protocols become standardized they may replace or be added to those already listed.

**RESTRICTED**: This class will be for special restricted usage. SSID broadcasts will be disabled, MAC filtering, and WEP Security should also be used. VPN may also be required. As new security protocols become standardized they may replace or be added to those already listed.

## V. Suggested Equipment Type and Manufacturer

*To be determined by the sub-committee and inserted here after evaluation of equipment and selection. (Ed note: probably should be included in a separate document so updating equipment list does not require Board approval.)*

## VI. Updates to this policy

Please address all questions and comments concerning this document to the District Technology Committee.