UCLA Minimum Connection Standards:

“Each device that connects to a network must meet minimum security standards. Standards must be reasonable and flexible to balance the requirements of people who use the network to conduct their duties with the responsibilities of those who protect the network and the devices connected to it. Standards must be broadly communicated, easily adaptable and widely accepted as reasonable”. (Excerpted from the UCLA Security Resolutions document adopted by the ITPB March 2004.)

Anti-virus Software

1) UCLA licenses, antivirus software for the UCLA campus. All members of the UCLA community shall install, activate and keep up-to-date antivirus software on all vulnerable computers including servers, email gateways, desktop computers, laptop computers and home computers connecting to UCLA networks.

2) While some systems may be immune from the effects of a virus, system administrators should recognize that each system can still send or transmit a virus to unsuspecting users.

3) If a system cannot support anti-virus software or if the user has other methods of achieving the same level of anti-virus protection, alternative methods of protection are acceptable as an exception.

Passwords

4) UCLA campus information service providers must have a suitable process for authorizing any use of information services under their control.

5) No campus electronic communications service user accounts shall exist without passwords or other secure authentication system, e.g. biometrics, Smart Cards. These measures must meet minimum complexity requirements: Contain at least eight characters, contain digits and punctuation characters as well as letters and not be a dictionary word.

6) All default passwords for network-accessible device accounts must be modified.

7) Passwords used for privileged access must not be the same as those used for non-privileged access.

No unauthenticated email relays

8) 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. Unless an unauthenticated relay service has been reviewed by CTS and approved as to configuration and appropriate use, it may not operate on the campus network.

No unauthorized Proxy services

9) Although properly configured proxy servers may be used for valid purposes, non-authenticated services commonly exist only as a result of inappropriate device
configuration. Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Unauthenticated proxy servers are not allowed on the UCLA network.

10) In particular, software program default settings in which proxy servers are automatically enabled must be identified by the system administrator and re-configured to prevent unauthenticated proxy services. For more information on the types of software typically used for proxy services see: http://spamlinks.openrbl.org/proxy-fix.htm.

**Departmental network devices**

11) All campus connectivity points (where organizations connect with the Campus backbone) will be maintained with the most reasonably current functional recommended up-to-date versions of operating systems and the security practices as defined by a “best practices” document updated according to changing technology and approved by CSG. Connectivity points will function as “chokes” or “governors” for securing campus traffic while introducing the least level of latency or “brittleness”. Network devices connecting to the campus backbone should be monitored for at a minimum, flow statistics. Departments must have the ability to identify sources of traffic and have the ability to control the flow of traffic from specific sources or disconnect specific sources.

**Patch Management**

12) Campus owned desktops under management by IT departments shall keep the computers up-to-date and patched to the level of critical security patches.

**Exceptions**

13) Anyone who wishes to connect to the UCLA network, but cannot meet minimum connectivity standards, may demonstrate to the NC or IT dept. head, they can achieve the same goals as set out in the minimum connectivity standards using other means of security.

14) Computers that are not institutionally owned or not part of the UCLA community such as visiting scholars represent an exception to these minimum standards and unit service providers may take necessary steps to secure departmental networks while allowing outside users.