

UCSD MINIMUM NETWORK CONNECTION STANDARDS

NOTE: These represent minimum connection standards only. Additional guidance to improve campus-wide network security is currently under development and will be issued at later date. More stringent standards may apply in individual campus departments.

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

1. Software patch updates

Campus networked devices must run software for which security patches are made available in a timely fashion. Consideration of patches available should be reviewed daily and applied as appropriate by each machine administrator. Some methodology must be in place to mitigate any security exposure if a patch is not applied. Such exceptions must be registered with Network Security; approved alternate means of securing the device may be necessary.

2. Anti-virus software

Anti-virus software for any platform currently listed on the Campus software distribution website (<http://software.ucsd.edu/>) must be running and up-to-date on every such device.

3. Unnecessary services

If a service is not necessary for the intended purpose or operation of the device, that service shall not be running.

4. Host-based firewall software

Host-based firewall software for any platform currently listed on the Campus software distribution website (<http://software.ucsd.edu/>) should be running and configured according to guidance provided by [Network Operations](#). The presence of an external access control mechanism does not obviate the need for host-based firewalls. Depending on the use of this device or data, additional protection may be required.

5. Passwords

Campus electronic communications service providers must have a suitable process for authorizing any use of shared restricted electronic communications services under their control. The mechanism for providing access to service users will be referred to here as an "account".

- a. No campus electronic communications service user accounts shall exist without passwords or other secure authentication system, e.g. biometrics, Smart Cards.
- b. Where possible, devices must be configured to enforce the aforementioned minimum password complexity requirements specified in the [Passwords](#) section of Network Operations site.
- c. All default passwords for network-accessible device accounts must be modified.
- d. Passwords used for privileged access must not be the same as those used for non-privileged access.

6. Minimize 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 surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all campus devices should use only encrypted authentication mechanisms.

In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP should be replaced by their encrypted equivalents wherever possible.

7. 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.

8. No uncontrolled-access to proxy services

Although properly configured unauthenticated proxy servers may be used for valid purposes, such services commonly exist only as a result of inappropriate device configuration. Open access proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Therefore, unless a proxy service has been approved by Network Operations as to configuration and appropriate use, it is not allowed on the campus network.

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 uncontrolled access to proxy services.

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 more than 20 minutes.

See <http://security.ucsd.edu> for additional details to assist system administrators and end-users to configure their networked devices.