

Los Angeles City College Administrative Services "How To" Book	Information Technology Department	IV H-6
How Do I Know if I can Access the Network Remotely?		

A. How Do I Know

How Do I know if I can access the network remotely?

1. The College (District) allows for Internet-based VPN access to the network resources. This is the only sanctioned method of remote network access. Connecting an unauthorized modem and a telephone line to any part of the network (including desktop workstations) is strictly prohibited and considered a serious breach of network security.
2. Remote network access is provided on an as-needed basis. Any employee or vendor who requires remote access to the network resources must have his or her direct supervisor submit a request form to the college administrator for approval. The employee/vendor will then be issued the following:
 - a. A security token for access to the network resources.
 - b. Required software for creating an encrypted VPN session over the Internet.
 - c. Directions for installing the VPN software.
 - d. Directions for accessing the network remotely.
3. The College does not accept responsibility for supporting the system which the employee or vendor plans to use for remote access. The employee or vendor agrees that by accepting the software, he or she is responsible for any and all upgrades required to support remote access. This includes (but is not limited to)
 - a. A telephone line.
 - b. A modem or network interface card.
 - c. A faster processor.
 - d. Additional disk drive space.
 - e. An Internet account with an Internet Service Provider.
 - f. A firewall or firewall software on the employee or vendor's remote system.
4. In addition, support for remote access will be provided by the ATS only for the internal network up to and including the network perimeter. The employee or vendor is

responsible for providing his or her own support for connectivity problems outside of this scope. The employee or vendor agrees to keep all information regarding remote network access confidential. The employee or vendor will not disclose password information or make copies of the VPN software; even for other employees or members of the vendor staff. Propagating remote access details is considered a security breach that cause substantial damage to the /College (District) WAN/LAN system. Ref: http://www.laccd.edu/admin_regs/ **Administrative Regulations B-28**