Are there any security requirements for connecting a device to the UCLA network?

Please see UCLA's Minimum Security Standards for Network Devices UCLA Policy 401

From: Associate Vice Chancellor Jim Davis, Office of Information Technology
Sent: Monday, July 17, 2006 6:00 PM
Subject: Minimum Security Standards for Network Devices

UCLA Office of Information Technology

Deans, Directors, Department Chairs and Administrative Officers

A minimum security standards policy for all devices connecting to the UCLA network has gone into effect as part of an ongoing initiative to enhance the security and privacy of UCLA's electronic data and resources. UCLA Policy 401 focuses on the security of individual devices connecting to the UCLA network â" including, but not limited to, laptop and desktop computers, printers, specialized medical and research instruments, and PDAs. Policy 401 articulates standards for software patch updates, anti-virus software, host-based firewall software, passwords, authentication, email relays, proxy services, and physical security. This policy is pursuant to the draft minimum standards policy that you were informed of in June 2005.

This policy has implications for faculty, non-IT staff, and students. Specifically, anyone who maintains a computer that connects into UCLA's network is responsible for compliance with this policy in order to connect. For example, a student, faculty or staff member who uses a personal computer in his or her home for work would be responsible for ensuring that the system complies with the minimum standards. A device that is not compliant or for which there is not a security plan may not be permitted to connect.

UCLA Computing Support Coordinators, Network Coordinators, Help Desk Consortium members, System Administrators and unit CIOs have a primary role and responsibility in the implementation, enforcement and ongoing support of this policy within their units. However, it must be understood

there are many devices for which the user, not the support staff, will have the primary responsibility for compliance.

The new policy was emphasized to departmental technologists in May in order to give them an opportunity to ask questions and make suggestions about the policy and its implementation. Many of the campus technologists were already familiar with the policy through their participation in working drafts circulated during the policyâ™s development and are now working to bring their units into compliance.

UCLA Policy 401 can be found at:

http://www.adminpolicies.ucla.edu/app/Default.aspx?&id=401.

Sincerely,

Jim Davis
Associate Vice Chancellor
Office of Information Technology

Revision #8
Created Thu, May 11, 2006 1:11 PM by Lee, Mike
Updated Tue, Dec 15, 2020 6:24 AM by William O'Brien