

College of Pharmacy Computer Use Policies - Networks

1. The Ohio State University College of Pharmacy, its employees and students, are subject to the University's Policies on Information Technologies. See: <http://cio.osu.edu/policies/> for guidelines on acceptable uses as well as prohibited activities.
2. No device will be connected to the College's computing networks without prior registration with the Technology Support Group. Information to be provided for registration will include the mac address(es) of the device, a hostname, the owner, the user, the location, and the operating system. Upon registration, the device will be assigned an IP address from among our College-administered sub-domains, and appropriate entries will be made to our Access Control Lists and DHCP client reservation servers. Updates to changed registration information will be provided by the user/owner as they occur. Owners with registered personal equipment will notify the Support Group on their departure from the College.
3. Devices which will be positioned behind a router/firewall on our networks will likewise be registered prior to connection.
4. Devices include but are not limited to: computers, notebooks, tablets, PDA's, access points, printers and routers. *Anything which can receive or transmit data over our Ethernet networks will be registered.*
5. In no case will an IP address be copied, moved, transferred, borrowed, guessed, or otherwise implemented without notification and approval of the Technology Support Group. Abuse of this policy may result in permanent loss of network services or confiscation of equipment.
6. If a temporary IP address is required (e.g. to facilitate connection of presentation hardware by a visitor), a preconfigured and registered router/firewall can be obtained on loan from the Technology Support Group. You are urged to plan ahead: early notification will ensure availability of this service.
7. All computers on the College networks will be maintained with current operating system patches and security fixes ("Critical Updates"). Updates are to be performed on a regular basis (weekly?) or as advised by the Technology Support Group (usually in the event of a new network assault). In the event that this is impractical (e.g., due to special interface requirements of instrumentation), the device will be positioned behind a user-provided router.
8. All accounts on computers connected to the College networks will have passwords, and the passwords will be selected so as to be rigorous and non-trivial.
9. All computers connecting to the College networks will have competent anti-virus software installed, and this software will be regularly updated (daily). Currently, the recommended software include Command Software (Authentium) CSAV for College-owned machines, and McAfee VirusScan licensed by OSU. In no case should multiple instances of anti-virus software be running concurrently on one computer.
10. It is strongly recommended that competent software to detect and block "spyware" and "adware" be installed and maintained. Currently *Spybot – Search & Destroy* is recommended.

11. In the event that a network connected device is found to have a worm, virus or other variant of malicious software, it is to be immediately disconnected from the network on instruction by the Technology Support Group, and remain so until the problem is cleared. Note: there is a possibility that some “malware” activities may result in the confiscation of hardware by campus or other security or law enforcement offices.
12. Any computer that will be enabled for hierarchical file sharing (e.g. ftp, http) must be registered and approved for this activity with the Technology Support Group. While the College does not currently prohibit peer-to-peer sharing *within its sub-domains*, such sharing to extramural sites is subject to review for security and appropriate use considerations. Sharing of copyrighted materials is expressly prohibited in accordance with University policies.
13. To facilitate maintenance and trouble-shooting of computers within the College, the Technology Support Group may request or require access to power-on passwords and/or creation of a secondary administrator account. In the event that such privileged access cannot be provided, the computer(s) involved may be prohibited from connecting to the College networks.
14. The security and integrity of any personal data on a computer connected to the College networks is entirely the concern and responsibility of the end user. Connection to our networks implies the user’s assumption of “acceptable risk”.
15. Ideally, patient data should be kept on computers ***not*** attached to our networks. Appropriate steps to safeguard data including strong passwords, data encryption, router/firewall barriers and access control lists should be employed. The Technology Support Group can advise users of patient data on these approaches but assumes no responsibility for the data security.