Cleveland State University

University Network Policy

Network Connectivity

1. Every CSU-owned PC will be a member of and authenticate against the CSUNET Domain, if possible.

2. All campus PC's will authenticate against the CSU Active Directory.

3. There will be only two authority levels in the University's wireless network:

   'guest access' - authentication will not be required
   Internet access only

   'full access' - be a member and authenticate against the CSU Domain
   get full 'wired' access

4. Independent deployment of wireless networks and products by departments or individuals can limit the accessibility and quality of service because of potential problems involving interference and capacity. IS&T will monitor the use of airspace for potential interfering devices and will notify a user if a device is causing interference and potentially disrupting the campus network. In these cases, IS&T reserves the right to restrict the use of all wireless network devices in University-owned buildings and outdoor spaces on the campus.

5. All new and modifications to network devices, voice communication and low voltage cabling must be coordinated through IS&T to insure such devices comply with national, state and local codes as applicable to wiring methods, construction and installation of data and communications cabling systems.

6. Only IS&T's Enterprise Network Department is authorized to place equipment or cabling in wiring closets, equipment rooms, etc. All communication closet access is granted through IS&T's Enterprise Network Department.

7. Because the data and voice communications network is a mission-critical and strategic University resource, devices other than computers, servers and workstations or authorized communication devices must not be plugged into any network or voice communication port. This includes, but is not limited to, hubs, switches, repeaters, routers, network modems, and wireless access points. These devices may be incorrectly configured and consequently be incompatible with existing network equipment and may cause outages and/or reliability problems. Devices not approved for use on CSU's data and voice communication network will be disabled to ensure the stability and availability of the

communications network.

8. Any machine or device found to be in violation of this policy is subject to be removed from the network.

9. Voice and data communications rooms are a vital part of the university communication network. These locations must remain a secured space that has very limited access to them. Access to these locations may only be authorized by Information Service & Technology, Enterprise Network Department.   No other equipment shall be installed in the communications rooms with out written authorization from the Information Services and Technology, Enterprise Network Department.

10. Information Service and Technology, Enterprise Network Department will insure that key latency-sensitive, critical business applications receive the bandwidth that is necessary to perform at their peak and will throttle less mission critical data.

REVISION HISTORY