

MCIS POLICY

SUBJECT: Unauthorized Network Hub, Switches and Wireless Access Points

SEE ALSO: Health Insurance Portability and Accountability Act (HIPAA) of 1996
 Hospital Policies: 01-14 – Management of Hospital PC Computing Resources
 01-15 – Electronic Data Security
 04-09 – Hospital Computer Equipment
 UK Administrative Regulations: 63 II-1.7-2 – Policy Governing Access to and Use of University of Kentucky Computing Resources

INFORMATION

The University of Kentucky became responsible for the installation and maintenance of its voice, data and video in 1986. At that time, a set of standards was adopted. Based on these standards Communications and Network Systems (CNS) has been responsible for the installation and maintenance of the University Network. The Hubs, Switches, Routers and all other equipment that make the Networking possible are chosen carefully. These devices are connected together via campus cabling infrastructure. The installation of the Network components are done according to design and engineering requirements, set forth by the campus Network Engineers at CNS. Based on this and the fact that the Network supports all Students, Faculty and staff, standards must be adhered to closely.

Due to recent terrorist incidents in this country a great deal of emphases has been put on the security of the Network. Additionally, for the Medical Center, protection of patient information is mandated to meet HIPAA Standards. The new ICIS system has to be put in place and operate consistently and reliably. A well-designed, installed and maintained Network is essential. With these requirements in mind, University of Kentucky Communications and Network Systems must establish restrictive policies and take the leadership role in enforcing the appropriate security measures and networking standards.

Therefore network devices or components that are installed by unauthorized (non-CNS) individuals are subject to removal and loss of service until the higher authority in that area/unit approves in writing and funds the correct method of installation.

Approved Devices:

Only devices that are selected by CNS Network Engineering staff and purchased through CNS are to be installed and connected to the campus network. Currently these devices are acquired from Cisco. Individually purchased mini-hubs and wireless access points are not permitted on the network without written CNS Management authorization.

Action:

When any unauthorized network device is found connected to the University Network,, CNS staff will submit a report to the respective unit (department head, College Dean and/ or Sector VP). Service to the unauthorized equipment will be terminated until CNS has been given in writing a request to make the installation correctly at the department's cost.