



**SUB-TOPIC
CAMPUS NETWORK CONNECTION POLICY**

All equipment connected to the UTD campus network (physically or wirelessly) must be associated with, and in support of, the mission of the institution. The integrity, security, and proper operation of the UTD campus network require an orderly assignment of network addresses and the correct configuration of devices attached to the network. Network access, performance and security can be put at risk when uncoordinated devices are introduced into the network environment. Therefore, all connections to the campus network need to be coordinated with accessibility, performance, and security concerns taken into account.

Information Resources (IR) is responsible for the campus backbone network, including routing, switching, domain name service, etc. It is the logical entity to coordinate all connections to the campus network including the assignment of unique addresses. Therefore, it is the policy of UTD that all devices connecting to the campus network be coordinated through IR (and assigned a network address if necessary).

Connection of equipment to the campus network is a privilege with concomitant responsibilities. Specifically, good network citizenship requires the timely updating of operating systems and virus protection software in order to minimize risks associated with computer hacking and other threats such as worms and viruses. Information Resources will endeavor to provide automated mechanisms to facilitate such updates to the extent reasonably possible. Campus entities that choose to opt out of such services are still obligated to perform the maintenance necessary.

Equipment found to be in violation of this policy may be disconnected and/or blocked from accessing the campus network without notice and may result in disciplinary action. This includes any device that negatively impacts or interferes with network operation, security or accessibility.