Network Devices	6-006 TECHNOLOGY SERVICES December 2019

POLICY

1.01 The OSU Institute of Technology (OSUIT) data communications network is a mission critical strategic university resource. Unsecured connections to network services can adversely affect the whole university. In order to protect the data communications network and the security of the information on it, devices other than computers and mobile communications devices must not be connected to the network. This includes, but is not limited to, hubs, switches, repeaters, routers, network modems, printers, appliances, and wireless access points unless approved in writing by Technology Services (TS). These devices may be incorrectly configured or incompatible with the university network causing outages and reliability problems to all or part of the network or may compromise the security of the information stored and in transit on the network.

PROCEDURES

2.01 Devices not approved for use on the university data communications network, or found to be disrupting the network, will be disabled to ensure the stability, confidentiality, integrity, and availability of the network. Network connectivity will not be restored until it is confirmed that the device has been approved or the misconfiguration corrected.

2.02 TS strives to provide high availability and stable network resources relevant to the OSUIT community's needs. Units needing additional network resources should make their request with the TS Service Desk.

2.03 All devices connected to the network must have up-to-date anti-virus and malware protection, a firewall configured to deny all incoming connections, and be secured with a complex password as outlined in OSUIT policy 6-004.

2.04 All connections to the computers and servers located on the university's internal network, from outside the network, must be routed through Cisco Anywhere VPN software. Other VPN software which opens ports in the computer's software firewall, to accept outside connections, is not allowed.

2.05 User ids, passwords or shared keys to wireless access points may not be shared.

2.06 Guests without an O-Key account must request a service account from the TS Service Desk or a guest account to access the network.

Approved: June 2005
Revised: July 2009
Revised: May 2013
Revised: July 2016
Revised: December 2019