Network Use Regulation

RUL08.10.03 Current Version

Authority: Vice Chancellor for Administration and Finance

History: ITCS Policy Number 1.601 Supersedes Policy Dated: September 26, 2003 Effective Date: November 1, 2011 Review Date: October 12, 2011 Placed in University Policy Manual after EXPEDITED REVIEW, transitioned without substantive change from prior version, March 25, 2013.

Related Policies: N/A

Additional Resources: Academic Computer Use Policy, University Student and Employee Computer Use Policy

Contact Information: Tom Lamb Director, IT Infrastructure Services 252-328-9008

1. Introduction

1.1 Purpose of Regulation

To establish guidelines governing the use and connection of networking devices on the University's Communications Networks. This policy applies to all University networked devices, ranging from multi-user systems to single user personal computers. Networking equipment includes, but is not limited to, switches, hubs, routers, firewalls, load balancing devices, proxy servers, wireless access points, blade server systems, Virtual Private Network (VPN) devices and/or devices requiring the trunking1 of Virtual Local Area Networks (LANs).

1.2 Person(s) with Primary Responsibility

Director of Network Services

2. Regulation

The University provides network access and capabilities through the Network Services Team of the Information Technology and Computing Services Department. The guidelines listed below are required in order to provide the University a reliable and stable networking platform

1 A trunk is a single transmission channel between two points that allows multiple virtual channels within the physical transmission channel, each point being either the switching center or the node.

3. Guidelines

All networking equipment connected to the University network must first be registered and approved by the Network Services Team of the Information Technology and Computing Services (ITCS) department. Devices requiring the trunking of Virtual Local Area Networks (VLANs) must be administered and managed by Network Services or a designated representative as authorized by the Director of Network Services.

Networking devices must be pre-approved by Networking Services, prior to purchase in order to ensure that the device will not have an adverse impact on ECUs network. Pre-purchase engagement works to limit the potential issues or conflicts from the acquisition. The responsible parties of problem network devices and/or services will be notified and expected to correct the problem in a timely manner.

Any networked devices or services that are detected and verified to degrade the quality of service on the network, if not corrected will result in termination of network service of that device until the cause of the problem is corrected. ITCS will assist users of authorized equipment in resolving the problems with their devices. Upon verification or certification of corrective action(s), the offending system will be re-admitted to the network.

Activities, which interfere with the operation of the network, are prohibited. These include but are not limited to the propagation of computer worms, network sweeps, network probing, network scanning, viruses, or Trojans.

4. Violations

Violations will result in the termination of network service to the offending network device and in the case of a willful violation be handled in accordance with the applicable Computer Use Policy. Network abuse will be referred to the Chief Information Officer.