UF UNIVERSITY of FLORIDA
Information Technology

POLICY

Policy: TS0008	Category: Technical Security	Version Date: 2/1/2017
Title: Network Security Authority and Responsibility Policy		Effective Date: 2/15/2017
Originating Unit: Information Security Advisory Committee		Last Review: 2/1/2017
Review Resp: HIPAA Security Officer		Next Review: 2/1/2020

Purpose:

The purpose of this policy is to specify the authority for network infrastructure access, implementation, or change.

Scope:

This policy applies to all HSC employees, contractors, and others using network services within the UFHealth network.

Reference:

1. UF Information Technology Security Policy http://www.it.ufl.edu/policies/
2. Internet Protocol Address Assignment Policy http://www.it.ufl.edu/policies/networking/ip-address-assignment-policy/

Policy:

1. Network Service Providers are the only entities authorized to:
    a. Implement, change or remove the network infrastructure. This includes, but is not limited to, basic network devices such as cabling, hubs, switches, routers, network firewalls, and wireless access points.
    b. Offer alternate methods of access to network resources such as modem pools for network access and virtual private networks (VPNs).
    c. Offer or delegate network infrastructure services such as DHCP and DNS.
    d. Manage the network IP (internet protocol) address space.
2. Users must not download, install or run security programs or utilities that reveal weaknesses in the security of an IT Resource unless they are authorized to do so by their Unit ISM and coordinated through the appropriate UF campus security administration.
3. All network connected equipment must be configured to a specification consistent with network service provider requirements.
4. All hardware connected to the network is subject to network service provider network management and monitoring standards.
5. The network infrastructure supports a well-defined set of approved networking protocols. Network service provider must approve any use of non-sanctioned protocols.
6. Vendor access to network resources must be coordinated with the network service provider in collaboration with the Unit Information Security Manager.

7. Failure to comply with this policy could result in loss of network access by the offending device and/or offending user.