UF UNIVERSITY of FLORIDA Health Science Center

Security Program for the Information and Computing Environment

Standard

Policy: TS0008.02	Category: Technical Security	Version Date: 2/15/2008
Title: IP Address Allocation and Use Standard		Effective Date: 4/01/2008
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 2/15/2008
Review Resp: HSC Chief, Information Security		Next Review: 2/2010

Purpose:

Internet protocol (IP) address space is an integral component of our network. IP address space is a limited resource needed by all HSC Units to enable network communications within and outside our network. IP addresses can be misused and abused thereby causing security threats to all network tenants. Therefore, IP address space needs to be regulated by the Network Service Provider for purposes of IP address availability and network security for all tenants of our network.

Scope:

This standard applies to all entities providing or managing core network services to any Health Science Center (HSC) Unit, and to the networked devices utilizing HSC address space.

Reference(s):

1. Policy GP0001: Applicable Information Security Regulations/Laws/ Policies.
2. Policy TS0008: Network Security Authority and Responsibility Policy.

Standards:

1. IP address space will be divided into ranges and assigned to certain network zones across our network. The following network zones will be implemented for HSC use for purposes of network optimization and access control that benefits all Units:
    a. Wireless Zone for authorized wireless device users and guests with authorized wireless devices.
    b. Voice over IP (VoIP) Zone for The Network Service Provider VoIP phones.
    c. Closed Zone for authorized devices that need to be prohibited from directly accessing the internet and from being accessed by devices on the internet.
    d. Protected Zone for authorized devices needing direct access to the internet but need to be protected from unsolicited and direct access by devices on the internet.
    e. Open Zone for authorized devices that need direct access to the internet and need to be able to be accessed directly by devices on the internet.
2. HSC Units may not circumvent the access controls of the network zones without approval from the Asst. VP Information Services/CIO.

3. Additional network zones will be evaluated, designed, and implemented as determined by the Network Service Provider. Primary consideration for additional network zones will be *HSC enterprise wide* need and applicability.
4. Maskable IP ranges will be created for designated HSC computer rooms. The Asst. VP Information Services/CIO or delegate will determine a designated HSC computer room based on number and size of HSC Units it services, and its compliance with SPICE Policy PS0002 Physical Security of Information Assets and Related Facilities and Standard PS0002.02 Physical Security of Server Rooms. The Asst. VP Information Services/CIO or delegate will maintain a list of the designated HSC computer rooms that will be eligible to receive maskable IP ranges. The Network Service Provider will arrange the maskable IP ranges for the designated HSC computer rooms with the IP Administrator.
5. The minimum registration information required to be eligible for public, private, static and dynamic IP address assignment is as follows:
    i. Machine name or DNS name
    ii. MAC address
    iii. Unit name
    iv. Device type (server, printer, desktop, portable, etc.)
    v. Network zone name
    vi. Name of registrar
    vii. Date registration information was last updated

   Devices that are not registered will be eligible for dynamic IP assignment in the HealthNet wireless security zone upon passing a security posture assessment and successful user authentication at the time of network access.
6. Device registration shall expire as follows:
    a. UF Managed registered devices – no expiration until deregistered by the Unit
    b. Unmanaged registered devices – annual expiration at end of UF spring semester

   Upon expiration, a device will no longer be able to access the network until it has been re-registered.
7. Registration information on all UF managed devices must be reviewed and updated by the Unit on a bi-annual (every two years) basis to ensure it is current and accurate.
8. Allocated static IP addresses that show no activity for more than 180 days may be reclaimed upon confirmation with the Unit that they are not being used.
9. The IP Administrator, designated by the Network Service Provider, will
    a. Maintain the authoritative source of IP address assignments
    b. Allocate and reclaim unused IP address space for the HSC Units according to this standard
    c. Manage access administration to the IP Administration system for HSC staff members per HSC authorization rules
    d. Provide the Network Service Provider with a reviewable report of authorized HSC IP Administration system users for annual renewal.
10. The Network Service Provider is responsible for
    a. keeping the IP Administrator informed and up to date with these standards

b. annually auditing the authorization of HSC staff for continued access to the IP Administration system and management functions
c. reviewing and approving HSC public IP requests
d. obtaining confirmation from HSC Units regarding unused IP space

11. All IP Administration system users
    a. must demonstrate a firm understanding of this standard by following it
    b. must ensure the appropriate network zone is selected based on the function and internet access control needs of a device
    c. are responsible for providing and updating the minimum registration documentation required for devices using IP addresses, as defined in this standard
    d. are responsible for the timely release of unused IP address space
12. HSC Unit ISMs are authorized to have access to the IP Administration system and management functions. The privileges the ISMs are authorized for are:
    a. Establish DHCP options for their group(s) of devices
    b. Authorize and establish IP administration user accounts for staff members in their Unit to register, deregister and update networked devices for their group(s)
    c. Register, deregister and update networked devices and acquire private IP addresses for the devices in their group(s)
    d. Request public IP addresses
    e. Release unused IP addresses
13. HSC Unit ISMs are responsible for the actions taken within the IP Administration system by the staff members whose accounts they have authorized.
14. HSC staff members who are authorized by their Unit ISM to have access to the IP administration system will have privileges for the following functions:
    a. Register, deregister and update networked devices and acquire private IP addresses for the devices in their group(s)
    b. Request public IP addresses
    c. Release unused IP addresses
15. Use of an IP address that is not assigned through the authoritative IP administrator may be an information security incident and will be handled as such.
16. Failure to comply with these standards could result in suspension of access to the designated IP Administration system and suspension of IP address growth until the Unit comes into compliance.