MEDICAL SCHOOL INFORMATION SERVICES
UNIVERSITY OF MICHIGAN

3rd Party Network Access UMHS Supported Buildings Recommendation for Management and Security

UMHS Wired TCP/IP Network:

Medical School Facilities – Research and Education Areas

- Network Provider – MCIT Network Services
- Wiring Provider – ITS - campus
- Construction Design Services – UM AEC
- Customer Coordination – primarily MSIS, some individual efforts
- Voice Services – ITS – campus
- Conduit and Environmental Work – UM Plant and 3rd party contractors.

UM Hospital Facilities – Clinical Care Areas

- Network Provider – MCIT Network Services
- Wiring Provider – AT&T
- Construction Design Services – UM Hospital Design
- Customer Coordination – primarily MCIT, some individual efforts.
- Voice Services – MCIT Telecommunication Services
- Conduit and Environmental Work – UM Facilities coordinating with UM Plant and 3rd. Parties

All third parties must use MCIT to access the Internet via a wired connection using the existing network infrastructure.

We see two options for providing wired network support to 3rd party companies they are similar across the enterprise:

1. One (1) Static IP/DNS name
   a. 3rd Party vendor has own switch and we only provide one IP port and address
   b. Port is on separate VLAN and on the 35.0.0.0 so it's routed directly to the Campus Bin and treated as being external to UM.
   c. Would need Administrative and technical contact from 3rd party for Internet usage complaints.
   d. Would use "private" VLAN and Virtual Routing and Forwarding (VRF) to provide separate and secure environment from UMHS network. This will require funding for switch code upgrade
   e. Downside is either these people get access to the comm. closet or suites that 3rd party people use need to be re-wired to alternate space (switch placed within the suite).

2. UMHS provides IP addressing/DHCP/DNS for all devices
    a. 3rd party devices are placed on VLAN on UMHS network switch
    b. UMHS provides static, DHCP, DNS for all 3rd party devices
    c. IP address range used is on 35.0.0.0 range and routed directly to Campus Bin and treated as external to UMHS.
    d. Would use “private” VLAN and Virtual Routing and Forwarding (VRF) to provide separate and secure environment from UMHS network. This will require funding for switch code upgrade
    e. No 3rd party access to communication closets
    f. MSIS would need to provided desktop support and troubleshooting (NCRC and Med School)
    g. Site-to-Site VPN would need to be set up to talk securely to UM resources
    h. Required more resources to configure and support

Wi-Fi or Wireless Issues:

MCIT is the only provider of wireless services using the 802.11 or Wi-Fi space across the health system. There are other spectrums or wireless areas that need to be documented, specifically cellular, emergency radio, telemetry, etc. (See other spectrum)

Because of the nature of the wireless spectrum, we do not see a way for 3rd parties to bring up their own wireless networks. There are both security and wireless spectrum bandwidth issues in allowing them to do so. If UMHS is to provide wireless networks to 3rd parties at NCRC or other buildings, we see two available options:

1. Guest wireless
    a. Terminated outside of Health System network
    b. Basic Internet
    c. No Security
    d. Least amount of support

2. Create Site Specific SSID
    a. PSK or 802.1x (if 3rd party has AD or authentication server)
    b. Terminates outside of Health System network
    c. Would provide secure wireless environment
    d. Significant support implications
    e. Device Support teams would have to support wireless clients
    f. Would have to have some kind of authentication based DHCP handout because a separate SSID could not be created for each 3rd party (system limitation and wireless bandwidth limitation.

Voice Services:

Medical School Facilities – Research and Education Areas – Voice services are provided by ITS and take several forms, traditional PBX, VOIP, Cellular, and a variety of voice application services.

- Network Provider – MCIT Network Services
- Wiring Provider – ITS - campus
- Construction Design Services – UM ACE
- Customer Coordination – primarily MSIS, some individual efforts
- Conduit and Environmental Work – UM Plant and 3rd party contractors.

UM Hospital Facilities – Clinical Care Areas – Voice services are provided by MCIT and take several forms, traditional PBX, VOIP, Cellular, and a variety of voice application services.

- Network Provider – MCIT Network Services
- Wiring Provider – AT&T
- Construction Design Services – UM Hospital Design
- Customer Coordination – primarily MCIT, some individual efforts.
- Voice Services – MCIT Telecommunication Services
- Conduit and Environmental Work – UM Facilities coordinating with UM Plant and 3rd. Parties

Internet Based Voice Services

Currently these services are enabled on all networks and monitored for bandwidth and security issues only.   These services are primarily customer/staff/student used with little organized deployment.

Cellular Services

Is public and does not impact this discussion, other than improving access. A large project is underway via RFP to select a potentially system for enhance cellular services with UMHS, progress of this process will be tracked

3. Vonage or Internet based phone service
    a. Telephone server comes in over the Internet.
    b. No UMHS support needed

Physical Security

We believe strongly that the physical security and integrity of the UMHS telecommunication closet infrastructure is paramount to assuring the integrity of the UMHS patient and corporate data. It is also essential to maintain this security to assured the ongoing operations of UMHS against accidental damage and disruption. To this end we recommend:

a. 3rd. parties not be allowed direct access to Telecommunication Closets and wiring plants
b. That access and services be maintained via use of UMHS managed resources or contractors that are certified and endorsed by MCIT networking services in coordination with the two major facilities providers, the IT support representative for the faculty (most likely MCIT or MSIS), authorized research administrator, or medical representative.
c. That no key or card reader access be granted to a 3rd party, unless they are governed by a contract relationship with the University of Michigan

If it is essential for a 3rd party to manage and control the wiring environment of the physical space that they manage, a separate telecommunication closer or cabinet should be deployed within the suite space and access to the Building Fiber, telecommunication or networking services should be routed to this location to maintain the integrity of UM and UMHS environments.

Deployment of Cabling

UMHS has maintained a strong discipline around managing the internal wiring of the facilities since about 1995. This disciplined was formed after several years of poorly managed wiring activity that led to significant service disruption, unnecessary expense, lack of standardization and poor collaboration. Having learned these lessons, UMHS has maintained a practice of standardizing the deployment and management of the cabling plant with UMHS. We recommend that that practice continue into the future.

To accommodate third parties, we believe that if a third party requires direct access to the communication wiring that this must be done in one of several ways:

a. Via a supervised process that assures the integrity of the facility.
b. Using one of the existing UM or UMHS supplied wiring/facilities services
c. By isolating the tenant from the physical wiring plant operating the building by constructing a private telecommunication closet within the 3rd party space.

Color Coding of Patch Cables:

MCIT, ITS, MSIS, UM Plant and UMH Hospital Facilities are currently working to an Enterprise Standard for cabling TCP/IP computer systems using the UM and UMHS networks to connect within the intra and Internet. The standard recommended colors are:

- Red – Medical Devices – Life Safety
- Green – Facilities Management Systems

- Yellow – Managed Devices – generally speaking workstations
- Blue – Voice Services or devices attached via VOIP Phones
- Purple – Research Instruments or devices
- Pink – Guest, 3rd party or Consumer Devices

Data Center or Server Environment

MSIS, ITS and MCIT recommend consolidation of Data Center facilities to the minimum number necessary to assure reasonable operational requirements for the mission of customers. The primary reason to place a server or storage equipment into a data center is to consolidate power, environmental, networking, security services and physical security of these assets.

We advocate the individual servers only be deployed outside of designated data center or specified locations when:

a. It is economically unfeasible to migrate the services
b. The nature of the technology does not allow it to run on an IP network
c. The nature of the technology requires close proximity to the customer, data collection instrumentation or another clearly defined requirement

3rd party services should not be physically attached to UMHS or UM networks without the interaction on a knowledge party who understand the technical, standard practice guide and operational implications of enabling these services. It is recommended that any deployment of these services should be reviewed before hand and that leasing documents or letters of understanding included essential components of the SPG and other contractual language protecting UM and UMHS technical environment.

Environmental Technology Scanning

UM policy requires MCIT and IT'S to regularly scan and report security, compliance and policy concerns quarterly to the respective compliance offices and at the direction of these offices will disable services upon direction. Also, in the event of the enterprise being disrupted by a services both ITS and MCIT will disable a services without prior approval of the customer if deemed appropriate at the time of the incident.

It are recommend that any 3rd party be required to acknowledge that this will happen and the they not being exempted from scanning unless the following conditions apply:

a. The design of their network integration does not use the UM or UMHS fiber plant, network or other services to operate
b. The design of their network is enabled by MCIT or ITS and that a written and approved agreement exists to allow the 3rd party to not be scanned.

3rd Parties granted Identity Rights by Authorized U of M parties

Thousands of non-U of M 3rd parties have been given access rights to UM and UMHS networks by authorized schools, individuals and organizations with UM and UMHS. If person has the following:

a. Unique Name
b. Kerberos or Level one Password

They will be able to establish connectivity to UM and UMHS networks with little barrier to entry. As such the credential in our environment act as the primary security barrier to network access. This method is one of the most likely methods that a third party will have to access the UMHS environment.   This is likely one of the easiest and best ways to provide services within the environment for authorized parties and should be first option for managing 3rd. parties with UMHS facilities, assuming that the relationship