MEHARRY MEDICAL COLLEGE **POLICIES**		**Page 1 of 6**
	Effective Date: January 31, 2008	
Retired:	**Revised: October 1, 2013**	

Approved by: A. Cherrie Epps, Ph.D.
President and Chief Executive Officer

A. Cherrie Epps PhD

Subject: Office of Information and Technology - Policy for Unapproved Campus Network Extensions

SCOPE:

The Vice President for Information Technology (VP) is designated as the institutional officer responsible for identifying standards for access and acceptable use of information technology resources.

POLICY STATEMENT:

The campus network serves the needs of the entire Meharry community. As a critical resource to that community, it is vital that it be managed in a professional manner. To facilitate that process, the campus network may not be extended without the express permission of the IT Department.

Applicability: This policy is applicable to all Meharry Medical College students, faculty and staff and to bona fide associates granted use of Meharry Medical College information resources. This policy refers to all College information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer communication facilities owned, leased, operated or contracted by the College. This includes cabling, servers, switches, hubs, routers, wireless access points and Internet access regardless of whether used for administration, research, teaching or other purposes.

PURPOSE:

Access to networks and computer systems owned or operated by Meharry Medical College imposes certain responsibilities and obligations on its users and administrators. Among these responsibilities and obligations is the requirement to protect Meharry resources from unauthorized network equipment.

DEFINITIONS:

Authorized Use: authorized use of Meharry Medical College owned, leased, operated, or contracted computing and network resources is used consistent with the education, research, and administrative mission of the College and is consistent with this policy.

Authorized Users: authorized users are (1) current students, faculty and staff of the College; (2) anyone connecting to a “public” Information Technology Station (ITS) or kiosk, and (3) others who have been authorized to use a particular resource by the campus unit responsible for operating that resource.

CO: Compliance Officer, the enforcing unit for the Computer and Network Usage Policies at Meharry Medical College.

MMC: Meharry Medical College (alias the College) for which the policy manual applies.

IT: Office of Information Technology, the source for establishing the Computer and Network Policies at Meharry Medical College.

Extensions: Extensions of the campus infrastructure fall into four main categories: extensions for the use of wired equipment using multi-port devices (hubs, routers, and switches); extensions for the use of wireless devices using wireless access points; extensions over leased lines or dedicated facilities to off-campus locations or other computer networks; and extensions through the telephone network to allow for remote access to College systems or services.

POLICY:

<u>Network Security Issues</u>

The College network must be kept secure. Security concerns involve protection of central data files, host computers and the network itself. Tracking of virus infections, compromised computers, and collaborating with other sites to isolate problems is an ongoing task. The technique most often used when problems occur is to quarantine the problem computer from the remainder of the College network by disabling its network port.

Clearly, a single-port model minimizes the interruption of services in a security incident. With network authentication, it will be possible to contact the person responsible for the computer to announce that the device has been quarantined, thereby saving time and confusion for the user.

Effects of Extending the Network on Network Security

When a single port is extended using a multi-port device then all computers connected through that port become subject to quarantine should any single one be compromised. Often, users will unwittingly place important service machines on multi-port devices along with less important workstations. When one of the workstations is compromised, then the server will lose network connectivity as a result of the quarantine procedure. This can immediately disrupt service for an entire department, research group, or students relying upon access to materials on that host.

When a compromise occurs on one of a group of hosts that are connected by a multi-port repeater (e.g. a device that offers no network isolation between hosts), then all hosts must be considered compromised and will need to be examined and repaired. This can require re-installation of the operating system and restoration of user files from backup for each machine at a significant loss of staff productivity and staff time.

Additional problems result from wireless access points. These devices are often poorly configured and may allow some level of access on the network to any passerby. If the passerby's computer is compromised, then it could operate as a vector for affecting other machines both on and off the wireless segment. The passerby may be connected to the network only briefly and other users may not be aware of the intrusion until it is too late.

Extending the campus network to remote facilities or interconnecting to other networks is a serious security hazard. Remote facilities may not have adequate security or appropriate terminating systems. Connecting an outside network to the College network undermines centralized firewall and intrusion detection.

Private modems on the infrastructure offer another mechanism through which a machine can be compromised. And as above, a modem compromise of machine can have a cascade effect throughout the web of other systems that trust that machine. Although surpassed in the press by the network-based hackers, unauthorized individuals using the telephone system and a modem are still a threat to host and infrastructure security.

Accountability

With increasing governmental regulations, the College must be able to document and account for network resource access and utilization. These regulations include:

- Protection of personal privacy, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Educational Rights and Privacy Act (FERPA),
- Security of systems that may be affecting other parts of the Internet, such as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), and
- Protection of intellectual property rights, such as the Digital Millennium Copyright Act (DMCA).

In addition, the College's own information systems are now designed to emphasize easy access to secure information for end users (e.g. Banner), which leads to increasing requirements to limit the possibility that information can be intercepted, inspected or modified in transit. Users who extend the infrastructure limit the College's ability to secure the information flow end-to-end and understand the security and bandwidth requirements of end systems.

Effects of Extending the Network on Accountability

Accountability relies upon authentication and secure transmission. All means of extending the campus network are potentially incompatible with this required end.

Private modem lines and private modem pools attached to the campus network are a vector whereby unauthorized individuals may be allowed access to resources, systems and information that the College has a requirement to secure and protect. The risk of leaking information through the use of private modems is high and has significant implications with respect to College compliance with government regulations.

Wireless access points present a similar accountability problem to modem lines. Without appropriate authorization and encryption, wireless access can be used to monitor traffic on the College network or to gain access to the network and its resources. Wireless access points can leave valuable and costly College resources, such as Internet connectivity, open to abuse by unauthorized persons.

Future use of the Infrastructure - Performance and Reliability

Individuals and groups throughout the College are actively developing applications and services that are becoming more dependent upon a deterministic network. The attributes of limited delay and limited jitter required by network-based video, network-based telephony, and other real-time applications, along with guaranteed, measurable service levels are rapidly increasing in importance for the business, educational and research operations of Meharry. The ability to manage the infrastructure out to the end device is increasing in importance to ensure that services can be delivered reliably and consistently.

Effects of Extending the Network on Performance and Reliability

Use of multi-port devices (hubs, routers, or inexpensive unmanaged switches) attached to the campus infrastructure blurs the deterministic nature of the infrastructure. For example, a user with a hub connected to a campus switched Ethernet port may not support the same high-quality video that a co-worker receives who is directly connected to a campus switched Ethernet port. While that co-worker may watch a video event without problems, others with multi-port devices could be prevented from doing so. The erroneous perception that this is a 'network' problem wastes time and resources and could affect the general impression of the College's infrastructure. Similar problems can occur when users on hubs attempt to use video conferencing. These devices do not adequately support the required protocols, thus diminishing service or in some cases preventing service altogether.

This problem will be compounded as Meharry has begun deploying VOIP (Voice over Internet Protocol) telephony services. With VOIP, it is likely that a user's computer will become an integral part of a general communication system, alerting the user to voicemail, providing directory and dialing services, and providing application sharing functions. Hubs will severely affect VOIP services and could be incompatible with its deployment. This continues to emphasize the importance of a single-port service model.

Wireless access, based upon common authentication and protocol support, is essential to transparent service across the College. Reliable service, in the eyes of the end user, must involve unified access, encryption and authentication. Islands of access resulting from network extensions are counter to this service model.

Network Operation Issues

Network support operations involve monitoring the network and solving individual repair cases as quickly as possible. As a business function, this support must be effective and cost efficient.

Effects of Extending the Network on Network Operations

Hubs and wireless extensions to the network are a short-term approach that can be very costly in lost local staff time and network operations time. The ability to assist users in troubleshooting problems with hosts connected to a hub is severely limited. There have been occasions where departments and research groups have been seriously affected while problems are sorted out. In order to determine the nature of the actual problem, the user is required to remove the multi-port device from the network.

If many users on a particular piece of the campus infrastructure are using hubs, then the cost to convert that set of users to single-port service may be significant due to compounded equipment, space and wiring costs. Departments that are systematically using hubs rather than purchasing needed ports are unfairly shifting the overall cost of the network onto other users. This shifting is compounded by the increased costs to troubleshoot multi-port connections should problems arise.

The argument that people who use these multi-port devices only hurt themselves is misguided. Experience has shown that hubs tend to fail in very unpredictable ways. Often these failures adversely affect other users within the same broadcast domain. Thus, the failure not only affects users on the multi-port device itself, but also other users on the same LAN.

As multi-port devices have begun to offer additional functions, such as DHCP and firewall services, configuration has become more complicated. Without understanding defaults and options, these devices are frequently installed in ways that disrupt the operation of the LAN for all users, which is often reported to IT as a network failure and is resolved only when IT staff locate the device and remove it from the network.

Conclusion

Based on these four issues - security, accountability, future network performance and reliability, and network operations - it is important that departments and divisions remove unauthorized extensions (hubs, unmanaged switches, routers, wireless access points and modems) from the College network in accordance with College policy. The removal will provide tangible benefits to the end users, will allow the College to maintain a secure and cost-efficient infrastructure, and will ensure a level of service that will support future technologies.

EXHIBITS: None.