SECTION: Information Technology **Number: 10.03.04**
AREA: User Guidelines

SUBJECT: Connecting Devices to University Networks

I. PURPOSE AND SCOPE

The purpose of this document is to promote secure and reliable networks for the university community by reducing the potential for connecting improperly configured or unsecured network devices and systems to the university networks. This document outlines the requirements for the use of network devices and systems and provides connection processes to the university voice, data, wireless or video networks or any interconnected local area network.

This document applies to any new or existing connection of any network devices or systems including, but not limited to, classroom technology equipment, servers, minicomputers, workstations, microcomputers, telephones, surveillance cameras, PDAs, etc., connecting into a university voice, data, wireless or video network by any university department, faculty, staff, student, guest or vendor. This document outlines the responsibilities for and process of requesting approval for connectivity to university networks.

II. POLICY STATEMENT

Each proposed connection must be approved by the Chief Information Officer or designee. This includes the advance review and approval of all design and engineering specifications involving or affecting university networks by Information Technology (IT) Department in order to confirm compliance with applicable university policies and industry standards.

Network Connection Agreements will be developed between IT and colleges or divisions requiring advanced network connectivity services to identify the responsibilities of each party. Network Connection Agreements will be approved by the Chief Information Officer or designee prior to their implementation.

III. DEFINITIONS

Definitions of terms used in this policy may be found in the Glossary of Information Technology Terms located in the Information Technology MAPP section at http://www.uh.edu/mapp/10/100000.htm.

IV. GENERAL PROVISIONS

A. University of Houston departments, faculty, staff or students may connect or contract with an outside vendor to connect any type of device or system to University networks through the standard process with IT provided forms. (see Sections V and VI below).

Colleges and divisions that wish to provide Internet access or network support services to individuals, organizations or other entities not directly affiliated with the University of Houston must have a provision in their Network Connection Agreement authorizing such activity.

All computer account owners, facility supervisors, system administrators and computer custodians requesting network connections should communicate user responsibilities to users of their systems and network as defined in this and related policies, including MAPP 10.03.01 User Responsibilities.

Given potential disruption to the network, departments must consult the IT Support Center before acquiring devices that connect to the network or provide or require advanced internet services.

B. All individuals requesting network connections will be given university security guidelines and MAPP 10.03.01 User Responsibilities.

Any device connected to a university network is subject to a hardware/software audit by the Department of Information Technology to safeguard against viruses, sniffers, intrusions or any other abnormalities in the device or system that may adversely affect the network.

Any device or configuration found to be noncompliant with this document or is adversely affecting the network is subject to disconnection until corrected. Such disconnection will be immediate and without prior notice when deemed necessary to preserve the operational integrity of the network. All network connections must be requested and implemented in accordance with this document.

C. At any point in the approval, connection or subsequent network use, the Chief Information Officer, Information Security Officer or designees may contact the connecting department with questions or problems.

D. In any cases of disagreement over permission to connect a device to the university network, the final decision rests with the Chief Information Officer or designee.

E. Questions regarding a connection and the appropriate approval process should be referred to the manager of network planning and development in IT. IT will return a copy of the request in a timely manner indicating approval or disapproval of the connection, together with copies of MAPP 10.03.01 and this document. Reasons for disapproval will be provided.

V. REQUESTING STANDARD NETWORK CONNECTIONS AND SERVICES

A. Requests for any network connections or services must be submitted to IT on an online Work Request.

B. IT will confirm, coordinate and provide notification of the Work Request to the contact person.

VI. REQUESTING SPECIALIZED OR NON-STANDARD NETWORK CONNECTIONS OR SERVICES

A. Requests for connecting specialized devices or making any type of non-standard connections to university networks must be submitted in writing to IT on a completed Work Request accompanied by a memorandum and include the following additional information:

1. The device to be connected;

2. The purpose of the device and connection;

3. If applicable, the name(s) of the individuals (vendors) involved in making the connection;

4. The name of the person in the department to contact with questions or problems related to the connection;

5. Copies of design or engineering specifications for any specialized device or system; and

6. Any additional information considered important and relevant to the security and performance of the network.

B. If the request is approved, IT will confirm, coordinate and provide notification of completion to the contact person. If the request is not approved, IT will provide recommendations for approved alternate solutions.

VII. PAYMENT FOR NETWORK SERVICES

Pricing for services has been established to recover costs.

VIII. REVIEW AND RESPONSIBILITIES

Responsible Party: Associate Vice President for Information Technology and Chief Information Officer

Review: Every 3 years, on or before September 1

IX. APPROVAL

John Rudley
Vice President for Administration and Finance

Donald J. Foss
Senior Vice President for Academic Affairs and Provost

Jay Gogue
President

Date of President's Approval: November 30, 2006

X. REFERENCES

UH System Administrative Memorandum 07.A.03 - Notification of Automated System Security Guidelines
Computing Facilities User Guidelines
Information Security Manual located in key offices and on UH Home Page at http://www.uh.edu/infotech/php/template.php?nonsvc_id=268
Federal Computer Security Act of 1987
Texas Penal Code Sections 33.01 - 33.05

Index terms: Networks
Connecting devices to university networks
Network security
Network