**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 unauthorized ~~connecting improperly configured~~ or unsecured network devices and systems providing network services on~~to~~ the university network~~s~~. This document outlines the process for provisioning of network services.~~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~~ the ~~new or existing~~ connection of any network device~~s~~ or system~~s~~ providing network services including, but not limited to, ~~classroom technology equipment,~~ servers, ~~minicomputers, workstations,~~ access points, routers, ~~microcomputers, telephones,~~ surveillance cameras, network cabling, ~~PDAs,~~ etc., ~~connecting into~~ to the~~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.~~

Connection of client devices not providing network services, such as laptops and mobile devices, are governed by MAPP 10.03.01 - Acceptable Use of Information Resources.

II. POLICY STATEMENT

Network service connections must be approved prior to any connection being made. Any exceptions to the established process ~~Each proposed connection~~ must be approved by the Chief Information Officer (CIO) or designee. This includes the advance review and approval of all design and engineering specifications involving or affecting university networks by ~~Information Technology (~~UIT~~)~~ ~~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 .~~

~~IV~~III. ~~GENERAL~~ POLICY PROVISIONS

A. University of Houston departments, faculty, staff or students may request to connect or contract with an outside vendor to connect ~~any type of~~ a network device or system providing network services to the ~~U~~university network~~s~~ through the ~~standard~~ following process: ~~with IT provided forms. (see Sections V and VI below).~~

1. Requests must be submitted to the appropriate College/Division Technical Manager (TM) and Information Security Officer (ISO) for approval.

2. Once approved at the college/division level, requests must be submitted to UIT through an online work request.

3. UIT will review the request and provide notification of the status of the request to the contact person. UIT may require additional information prior to approval of the work request.

B. Network service agreements may be required between UIT and colleges/divisions requesting advanced network services identifying the responsibilities of each party. ~~N~~These network service agreements will be approved by the CIO or designee prior to their implementation.

C. 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~~ services 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.~~

D. ~~Any~~ All devices connected to ~~a~~ the university network ~~is~~ are subject to a hardware/software audit ~~by the Department of Information Technology~~ to safeguard against ~~viruses~~malware, sniffers, intrusions or any other abnormalities in the device or system that may adversely affect the network. The connecting department is required to provide any information requested by the chief Information Security Officer or designee.~~.~~

E. 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~~ may be made ~~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.~~

F~~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~~ CIO 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.~~

IV. WIRELESS NETWORK

All wireless network access point devices shall be provided by UIT. Any exceptions must be authorized by UIT through the process outlined in Section III. All wireless access points must meet the following requirements:

1. All wireless access point devices must be registered by UIT. UIT regularly performs building-to-building assessments to detect unauthorized wireless access point devices.

2. The wireless router or access point administration interface must be secure. The default password must be changed to be a strong password as described in MAPP 10.05.01 - Information Security Program. Guest access or accounts should be disabled.

3. The SSID must be changed from its default. Naming convention information is located on the UIT web site.

4. The strongest form of encryption should be used. Encryption of at least 128 bit must be enabled on the access point.

5. Wireless administration must be disabled. Access points should only be administered via a wired connection.

6. Confidential and sensitive personal information is prohibited from being transmitted over wireless network devices unless an encryption method such as Virtual Private Network (VPN) is utilized.

V. ~~PAYMENT FOR~~FUNDING OF NETWORK SERVICES

T~~Pricing for services has been established to recover costs.~~he network services funding model allows UIT to pass on substantial cost savings, helping our clients use university financial resources as efficiently as possible. The funding model offers predictability in cost by providing a single bundled rate for service that is set annually for the entire school or administrative unit, based upon the amount of service used. Service delivery models will ensure subscribers get all essential features and functions without the time-consuming and costly á la carte ordering and billing.

VI~~II~~. REVIEW AND RESPONSIBILITIES

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

Review: Every three years~~,~~ on or before September 1

VII~~IX~~. APPROVAL

~~John Rudley~~
Executive 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~~

## REVISION LOG

| Revision Number | Approved Date | Description of Changes |
|---|---|---|
| 1 | 07/12/1996 | Initial version |
| 2 | 11/30/2006 | Applied new MAPP template. The contents were updated to reflect current technology terminology and usage, such as computer networks and the Internet, and to reflect Information Technology department organizational changes and responsible reviewers and approvers. |
| 3 | TBD | Applied revised MAPP template and added new Revision Log. Removed Section III definitions. Contents have been updated to reflect current processes. Added Section IV on Wireless network information. Removed Sections V and VI on Requesting Specialized or Non Standard Connections or Services. Removed References and Index Terms. |