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

SUBJECT: Connecting Devices to University Networks

I. PURPOSE AND SCOPE

The purpose of this policy is to promote secure and reliable networks for the university community by reducing the potential for unauthorized or unsecured network devices and systems providing network services on the university network. This policy outlines the process for provisioning of network services.

This policy applies to the connection of any network device or system providing network services including, but not limited to, access points, routers, switches, firewalls, VPN, DNS servers, network cabling, etc., to the university network by any university department, faculty, staff, student, guest or vendor. This policy does not apply to end-user client devices such as desktops, laptops, tablets, etc.

Embracing the principle of Bring Your Own Device (BYOD), end users are responsible for compliance with MAPP 10.03.01 - Acceptable Use of Information Resources when connecting client devices such as laptops and mobile devices to university networks.

II. POLICY STATEMENT

Network service connections must be approved prior to any connection being made. Any exceptions to the established process 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 University Information Technology (UIT) in order to confirm compliance with applicable university policies and industry standards.

III. POLICY PROVISIONS

A. University of Houston departments, faculty, staff or students may request to connect or contract with an outside vendor to connect a network device or system providing network services to the university network through the following process:

1. Requests should 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 should 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 within 21 calendar days of submission. UIT may require additional information prior to approval of the connection request.

B. Service Level Agreements may be required between UIT and colleges/divisions requesting the connection of a network device identifying the responsibilities of each party. These Service Level Agreements will be approved by the CIO or designee prior to their implementation.

C. Colleges and divisions that wish to provide network services to individuals, organizations or other entities not directly affiliated with the university must have a provision in their Service Level Agreement authorizing such activity.

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

E. Any device found to be adversely affecting network performance or security is subject to disconnection. Such disconnection may be made without prior notice when deemed necessary to preserve the operational integrity or security of the network.

F. In cases of disagreement over permission to connect a device to the university network, resolution will be achieved through the standard university hierarchy.

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.

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 a secured wireless network or an encryption method such as Virtual Private Network (VPN) is utilized.

V. REVIEW AND RESPONSIBILITIES

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

Review: Every three years on or before September 1

VI. APPROVAL

Jim McShan
Senior Vice President for Administration and Finance

Renu Khator
President

Date of President's Approval: August 8, 2016

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	08/30/1996	Initial version (Original version was a Policy and a Procedure)
2	11/30/2006	Applied new MAPP template. The policy and procedure were combined into one document. 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	10/19/2011	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
4	08/08/2016	Revised Section I on network devices and Bring Your Own Device (BYOD) rules. Added 21 calendar days of submission rule to Section III.A.3. Revised Section III.F on resolutions being achieved through university hierarchy. Removed information in Section IV.3 that naming convention information is located on the UIT web site. Removed Section V