University *of* New Haven

Policies and Procedures

Policy Title: Office of Information Technology Wireless Security Access

Policy No.: 7020 Rev.: 0
Effective Date: October 8, 2019
Last Revision: October 8, 2019

Responsible Office: Office of Information Technology
Responsible Official: Associate Vice President for Technology & CIO

Contents

Scope

This policy applies to all the University of New Haven’s employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize university-owned, personally-owned, or publicly-accessible computers to access the organization’s data and networks via wireless means

Policy Statement

Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment at The University of New Haven does not automatically guarantee the granting of wireless access privileges. Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data. Addition of new wireless access points within corporate facilities will be managed at the sole discretion of OIT. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organizational campus, are strictly forbidden. This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

Reason for the Policy

The purpose of this policy is to define standards, procedures, and restrictions for connecting to the University of New Haven's internal network(s) or related technology resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

- External hosts via remote access technology (for example, using a wireless router at home to connect to the corporate Virtual Private Network).
- Wireless gateways on corporate premises.
- Third-party wireless Internet service providers (also known as "hotspots").

The policy applies to any equipment used to access university resources, even if said equipment is not university-sanctioned, owned, or supplied. For example, use of a public library's wireless network to access the corporate network would fall under the scope of this policy.

The overriding goal of this policy is to protect the University of New Haven's technology-based resources (such as data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing university technology resources must adhere to university-defined processes for doing so.

Definitions

Access Point
A stand alone device that connects to a wireless LAN

Encryption
A process which is applied to text messages, or other important data, to alter it in order to make it unreadable, except by someone who knows how to decrypt it.

OIT
Office of Information Technology.

Bandwidth
Refers to how much data you can send through a network connection. It is usually measured in bits per second.

Network
A group of two or more computer systems linked together.

Hotspot
The geographic boundary covered by a Wi-Fi (802.11) wireless access point.

VPN
A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Policy Sections

7020.1 Supported Technology

All wireless access points within the University firewall will be centrally managed by the University of New Haven's OIT and will utilize encryption, strong authentication, and other security methods at OIT's discretion. Although OIT is not able to manage public wireless resources, end-users are expected to adhere to the same security protocols while utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

The following table outlines the University of New Haven's minimum system requirements for a computer, workstation or related device to wirelessly connect to the

University of New Haven's systems. Equipment that does not currently meet these minimum requirements will need to be upgraded before wireless connection can be sanctioned by OIT.

	PC and PC-Compliant Computers	Macintosh Computers	Handhelds, PDAs and Portables
Operating System(s)	Windows 2000/XP	OS X	TBD
CPU (Type, Speed)	PIII, 1GHz	G3, 450MHz	
RAM	256MB	256MB	
Disk Space	20MB	0MB	
Wireless NIC Type(s) (Manufacturer/Model #)	Cisco, LinkSys, NetGear	Apple, Cisco, Linksys, Netgear	
Wireless Standard(s) (802.11a, b, g, or other)	802.11b, g	802.11b, g	

7020.2 Policy and Appropriate Use

It is the responsibility of any employee of the University of New Haven who is connecting to the organizational network via wireless means to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection used to conduct university business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

1. General access to the organizational network through the Internet by residential remote users through the University of New Haven's network is permitted. However, both the employee and his/her family members using the Internet for recreational purposes through university networks are not to violate any of the University of New Haven's Internet acceptable usage policies.

2. Employees using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with the University of New Haven's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if university work is conducted from home.

3. All remote computer equipment and devices used for business interests, whether personal - or university-owned, must display reasonable physical security

measures. Users are expected to secure their university-connected machines when they are physically at their machines, as well as when they step away. Computers will have installed whatever antivirus software deemed necessary by the University of New Haven's Office of Information Technology. Antivirus signature files must be updated in accordance with existing company policy.

4. Due to the potential for bandwidth conflicts within the university campus, use of unsanctioned equipment operating within the 2.4 GHz range is highly discouraged. If you have a need to use such equipment – for example, a wireless phone – please consult OIT before proceeding further.

5. Remote users using public hotspots for wireless Internet access must employ for their devices a university-approved personal firewall, VPN, and any other security measure deemed necessary by the OIT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with the University of New Haven's additional security measures. OIT will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.

   - Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, war drivers, and eavesdroppers.
   - Users must apply new passwords every business/personal trip where university data is being utilized over a hotspot wireless service, or when a university device is used for personal Web browsing.

6. Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access the University of New Haven resources must adhere to the authentication requirements of the University of New Haven's OIT department. In addition, all hardware security configurations (personal or university-owned) must be approved by the University of New Haven's OIT department.

7. Employees, contractors, and temporary staff will make no modifications of any kind to university-owned and installed wireless hardware or software without the express approval of the University of New Haven's OIT department. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware, or security configurations, etc.

8. Employees, contractors, and temporary staff with wireless access privileges must ensure that their computers are not connected to any other network while connected to the University of New Haven's network via remote access.

9. In accordance with the University of New Haven's security policies, sessions may time out after 3 minutes of inactivity, and may terminate after 2 connection status

failures in a row. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter university networks through a wireless connection.

10. The wireless access user agrees to immediately report to his/her manager and the University of New Haven's Office of Information Technology any incident or suspected incidents of unauthorized access and/or disclosure of university resources, databases, networks, and any other related components of the organization's technology infrastructure.

11. The wireless access user also agrees to and accepts that his or her access and/or connection to the University of New Haven's networks may be monitored to record dates, times, duration of access, data types and volumes, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

12. OIT reserves the right to turn off without notice any access port to the network that puts the university systems, data, users, and clients at risk.

7020.3 Enforcement

Failure to comply with the Wireless Security Access Policy and Agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.