

Wireless Policy

1. Purpose

The purpose of this policy is to secure and protect the information assets owned by Ithaca College. Ithaca College provides computer devices, networks, and other electronic information systems to meet its mission, goals, and objectives. Ithaca College grants access to these resources according to an individual's role and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy in order to connect to the Ithaca College network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by Information Technology Services are approved for connection to the Ithaca College network.

2. Scope

This policy addresses the requirements of Wireless deployments, Wireless usage, and Wireless airspace usage. All employees, students, contractors, consultants, temporary workers, and others who use the Ithaca College network, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Ithaca College, must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to the Ithaca College network or reside at an Ithaca College owned, leased or rented site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

3. Policy

Wireless Deployments

Standards supported:

- IEEE 802.11n is the preferred wireless networking standard. 802.11g, 802.11b, and 802.11a will be available, where necessary.
- IEEE 802.1X is the authentication standard. Additional security procedures may be applied as needed.
- WPA2 with AES encryption will be the only secure standard used.

Service Set Identifier (SSID)

There shall be two SSIDs broadcast by the wireless deployment.

- ICAirnet – For visitor Internet access and access to installation instructions and tools needed to access ICAirnet-Secure (see below).

- ICAirnet-Secure – For roles-based access to the network. Only devices authenticated via Ithaca College account credentials may access this SSID.

Wireless Service Considerations:

- Wireless networking has bandwidth limitations compared to the wired network. The wireless network should be viewed as augmenting the wired network, to provide more flexible network use. Applications that require large amounts of bandwidth, or are sensitive to changes in signal quality and strength may not be appropriate for wireless access.
- Wireless technology is and will for the foreseeable future be a shared bandwidth technology. Some protocols and services will not effectively work in, or may be inappropriate for, a wireless environment.
- Wireless IP Addresses
- DHCP is the standard addressing method for the IC wireless networks, and is expected to meet the majority of customer requirements.
- Wireless is a dynamic service. Due to the dynamic nature of wireless, IP space serving the campus will change over time due to capacity re-engineering.

Restrictions

Ithaca College policy requires that all deployments of wireless infrastructure be installed and maintained by ITS. Installing departmental or do-it-yourself wireless access points is prohibited to avoid possible interference with the IC wireless network, unnecessary impact to the wired network and to minimize undue security risks to the College. Additionally, in areas where centrally-managed wireless networking is available any pre-existing locally managed access points must be removed.

- Use of the wireless network is subject to the established policies for use of IC campus network services. (e.g. All College Computer and Network Use Policy)
- Only devices authenticated via Ithaca College account credentials may access network resources on the IC network that are not Internet facing.
- Unauthenticated visitors will be able to access only the Internet by accepting the policy restrictions on usage and providing their email address.
- Wireless Usage
- Authenticated Access

Role-based access to the network shall be established using the user's Ithaca College account credentials. All data transactions shall be encrypted and secured by the protocols listed in the Supported Standards section above. Services allowed through the wireless network should be substantially identical to those for wired access. Role based users will be limited to those same services they are permitted to access via wired network controls.

Visitors

Visitors shall have free access to the Internet only. They shall be limited to only those TCP/IP protocols listed in Table 1. In general, standard Web access, Secure Shell access, Instant Messenger access, email access, sending email via secure methods, and Remote VPN access are permitted by these protocols.

Source	Destination	Service	Action
Guest Wireless VLAN	All	HTTP	allow
Guest Wireless VLAN	All	HTTPS	allow
Guest Wireless VLAN	All	SSH	allow
Guest Wireless VLAN	All	AIM/5190/TCP	allow
Guest Wireless VLAN	All	YAHOO/5050/TCP	allow
Guest Wireless VLAN	All	MSN/1863/TCP	allow
Guest Wireless VLAN	All	Google Chat/443/TCP	allow
Guest Wireless VLAN	All	iChat/5190, 5298/TCP	allow
Guest Wireless VLAN	All	POP	allow
Guest Wireless VLAN	All	IMAPS	allow
Guest Wireless VLAN	All	IMAP	allow
Guest Wireless VLAN	All	SMTPS	allow
Guest Wireless VLAN	All	All ports needed for PPTP	allow
Guest Wireless VLAN	All	All ports need for IPSEC	allow
Guest Wireless VLAN	All	All	drop

Device support

All supported PDAs and Laptops shall be able to, at a minimum, access the Internet through the Visitor role.

Wireless Airspace

To provide wireless access, the radio frequency airspace of the campus serves as the transport medium for this technology. Wireless networks operate on the campus shared and finite airspace spectrum. Therefore, Information Technology Services (ITS) will regulate and manage this airspace centrally to ensure its fair and efficient allocation and to prevent collision, interference, unauthorized intrusion and failure. In addition, central management will facilitate the adoption of new features. Persons using wireless devices to connect to the College network must be aware of this, and comply with this policy and any other related policies.

ITS will approach the shared use of the wireless radio frequencies in the same way that it manages the shared use of the wired network. Specific issues pertaining to wireless network devices are outlined below:

- All access points will be installed and configured in such a way as to comply with all security features of the wireless network, including restrictions to provide connections only to those users who are entitled to access.
- The College reserves the right to remove, disconnect or electronically limit any access point not installed and configured by ITS personnel or specifically covered by prior written agreement and/or arrangement with ITS.
- Other devices such as portable phones, and wireless devices using "Bluetooth" (a competing wireless technology), that broadcast and receive information on the same frequency as wireless Ethernet devices may cause interference with wireless network operation. If disruptions in wireless service are reported, ITS will investigate and can remove any devices it deems, in its sole discretion, to be interfering with proper network operation.
- Only users affiliated with Ithaca College are authorized to use wireless networking on campus. To help protect these affiliated users from unauthorized access to their computer resources, ITS may implement data encryption and authentication security measures that must be followed by all users. These measures require the use of specific wireless LAN product types and are designed to meet emerging wireless encryption and security standards.

4. References

SANS (SysAdmin, Audit, Network, Security) Institute "Wireless Communication Policy" URL:
http://www.sans.org/resources/policies/Wireless_Communication_Policy.pdf

Villanova University "Wireless Policy" URL:
<http://www.villanova.edu/unit/policies/wireless.htm>

University of Massachusetts Amherst "Wireless Airspace Policy" URL:
<http://www.oit.umass.edu/policies/wireless.html>

University of Washington "UW Wireless Policy" URL:
<http://www.washington.edu/computing/wireless/policy.html>

Cornell University "RedRover-Guest Wireless" URL:
<http://www.cit.cornell.edu/redrover/guest.html>