Unauthorized Wireless Access Point Policy

Institute for Advanced Study

December 15, 2011 (revision 224)

Contents

1 Executive Summary

The Institute for Advanced Study (IAS) provides wireless (802.11) network access to its Faculty, Members, Visitors and Staff during their stay on our campus.

In order to ensure minimal interference, and to protect the Institute from unregistered users, we do not allow the operation of unauthorized, personal access points[1] on our campus.

2 Purpose and Scope

The purpose of this this Policy is to document that the operation of non-authorized, personal access points at the Institute for Advanced Study is not allowed. This policy covers all areas in which IAS computing provides network access.

2.1 Definition of Unauthorized Access Point

An Unauthorized Access Point is a wireless network device that has been installed without explicit authorization from the Institute for Advanced Study's Network Administration department.

2.2 Negative Impacts of Unauthorized Access Points

There are multiple reasons why Unauthorized Access Points are not allowed on the IAS campus.

2.2.1 Interference

Since Unauthorized Access Points use the same radio frequencies as our wireless infrastructure, they create radio interference. This interference negatively impacts the speed and reliability of our wireless network. In order to provide the best service possible for our users, we need to be able to control the frequency and power of all access points on our campus.

2.2.2 Unauthorized Access and Licensing

In order to remain compliant with existing and future licensing agreements, as well as to maintain industry best practices, access to the IAS wireless network requires user registration. Since Unauthorized Access Points can potentially bypass this requirement, we are unable to allow them on our network at this time, or we risk violating the terms of important service agreements.

2.2.3 Data Theft

An Unauthorized Access Point could be used in a malicious manner to deceive clients into connecting to it. This could lead to the theft of data sent over the wireless connection from unsuspecting clients.

2.2.4 Confusion

By adding more wireless networks to connect to, it could lead to the confusion of our users. We strive to make our wireless network as user friendly as possible, Unauthorized Access Points could derail this effort.

[1] Rogue Access Points (APs)

2.3 Lack of Coverage

If there is a lack of coverage in the area where the unauthorized access point is installed, Network Administration will work to cover the area with authorized equipment.

2.4 Lack of Feature

If there is a feature that the user needs, for example, a backup device[2] that by default is configured as a wireless access point, Network Administration will work to find an alternative method for the user.

3 Removal of Unauthorized Access Points

When an unauthorized access point is discovered, Network Administration will attempt to find the owner and have them remove the access point.

3.1 Notification of User

When contact information is available, Network Administration will email the owner of the Unauthorized Access Point requesting that it be shut down. If the owner does not respond, a second email and/or a telephone call will be made.

Once the owner has been contacted, they will be given one week to remove the device from the network.

3.2 Removal of Unauthorized Device

If Network Administration is unable to contact the user, if the unauthorized device is negatively impacting the IAS network, or if the user is unwilling to remove the device, the device will be removed from the network by Network Administration.

This may involve shutting down a physical port, or containing the device through wireless means, including disassociating clients connected to the unauthorized device. It also may mean gaining physical access to the device to remove it from the network.

When possible, Network Administration will attempt to let the user know that the device is going to be removed. It will also notify the Administrative Officer of user's school or Human Resources, if the user is a staff member.

4 Enforcement of This Policy

Network Administration is responsible for enforcing this policy.

5 Changes to The Policy

The Strategic Planning Committee (SPC) is responsible for maintaining the *Unauthorized Network Device Policy.* The SPC must notify computing staff of changes to the *Unauthorized Network Device*

[2] Apple Time Capsule is an example

Policy. The SPC may make changes to *Unauthorized Network Device Policy* whenever necessary, but shall review the *Unauthorized Network Device Policy* annually.

6 Related Documents

All Institute Computing policies can be referenced here: `https://security.ias.edu/policies`

- Institute for Advanced Study. *Unauthorized Network Device Policy*
- Institute for Advanced Study. *IAS Time Capsule Approved Installation Howto*
- Apple. *Time Capsule*