The University of the South Pacific

Serving the needs of the Cook Islands, Fiji, Kiribati, Marshall Islands, Nauru, Niue, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu and Vanuatu

Wireless Access Point Policy

Purpose

The purpose of this policy is to limit and restrict the number of wireless access points connecting to University of the South Pacific's internal network or related technology resources via any means involving wireless technology.

The overriding goal of this policy is to protect University of the South Pacific'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 USP technology resources must adhere to defined processes for doing so, using USP-approved access points.

Scope

This policy applies to all University of the South Pacific users, including full-time staff, part-time staff, contractors and students who utilize mobile computers to access USP's data and networks via wireless means. Wireless access to USP network resources is a privilege, not a right. Consequently, a user at University of the South Pacific does not automatically guarantee the granting of wireless access privileges.

This policy is complementary to any previously implemented policies dealing specifically with network access and remote access to the enterprise network.

Access Points

University of the South Pacific is committed to providing authorized users with wireless access to the Internet, University of the South Pacific networks and systems, as well as other resources. In order to make this convenient service available to end users, IT Services must install "access points" in and around the premises wherever wireless access to USP resources is designated. These access points are generally small, antenna-equipped boxes that connect directly to the local area network (LAN), converting the LAN's digital signals into radio signals. The radio signals are sent to the network interface card (NIC) of the mobile device (e.g. laptop, etc.), which then converts the radio signal back to a digital format the mobile device can use.

- As the number of wireless connections increases, so too does the danger of "rogue" access points being surreptitiously installed. Rogue access points are antennas that are installed without the knowledge or permission of University of the South Pacific, used by hackers, internal employees, or trespassers to gain illegal access to the company network and Internet connection for the purposes of sabotage, spamming, corporate espionage, personal gain, and so on.

- All wireless access points within the USP firewall will be centrally managed by University of the South Pacific's IT Services and will utilize encryption, strong authentication, and other security methods at IT Services discretion. Addition of new wireless access points will be managed at the sole discretion of IT Services.

- Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organizational premises, are strictly forbidden.

Policy Restrictions

1. University of the South Pacific uses the 802.11[…] protocol as its wireless network standard, transmitting at the choose 2.4 GHz radio frequency spectrum, with the intention of delivering speeds of up to 54 Mbps to mobile and wireless devices.

2. University of the South Pacific's IT Services will support only the following devices and equipment for accessing corporate networks and systems wirelessly:

    - Access Points installed by the IT Services (ITS) department
    - Cisco and Cisco-compatible client devices
    - Laptop computers using Windows 2000 and XP operating systems or Macintosh OS 10.3.3 and above

3. The IT Department will strive to purchase only those access points and equipment that possess the following characteristics and/or features:

    - RADIUS authentication
    - SNMP
    - Syslog
    - WPA encryption or 802.11i-compliant
    - Power-over-Ethernet (PoE)
    - Backward-compliant with 802.11b (if product is 802.11g)
    - High plenum rating, fire-resistant
    - Wide temperature range for outdoor use
    - Anti-theft physical security measures.

4. All wireless clients and devices shall be equipped with a host-based personal firewall and anti-virus software. The user shall update these applications as required, and will not reconfigure them in any way.

5. Whenever necessary, the IT Services will conduct a site survey to determine the appropriate placement of new or additional access points. All installations will be in compliance with all local safety, building, and fire codes.

6. All wireless access points, including those designated for networking home offices or satellite offices with the USP network, must be approved by University of the South Pacific's IT Director.

7. All access point broadcast frequencies and channels shall be set and maintained by the IT Department. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.

8. Use of the wireless network is subject to the same guidelines as University of the South Pacific's technology and Internet acceptable use policies.

9. All data that traverses the USP wireless network must be encrypted, using Wi-Fi Protected Access (WPA) at minimum. IT Services will strive to procure only WLAN equipment that supports WPA, and will also provide suitable software for authentication and encryption.

10. IT Services cannot guarantee 99.999 percent availability of the wireless network, especially during inclement weather. Nevertheless, IT Services will make all possible network adjustments within the supported radio frequency spectrum.

11. IT Services will conduct sweeps of the wireless network to ensure there are no rogue access points present. Empty rooms and offices will also have their network jacks disconnected from the switch in order to mitigate rogue access point installation.

12. IT Services reserves the right to turn off without notice any access point connected to the network that it feels puts USP's systems, data and users at risk.

13. The wireless access user agrees to immediately report to IT Services any incident or suspected incidents of unauthorized access point installation and/or disclosure of company resources, databases, networks, and any other related components of USP's technology infrastructure.

14. Any questions relating to this policy, as well as any help desk inquiries, should be directed to the IT helpdesk at telephone number 323 2117 or email: helpdesk@usp.ac.fj.

Policy Non-Compliance

Failure to comply with the Wireless Access Point Policy and subsequent agreement may result in the suspension of remote access privileges and disciplinary action.