Southern Response
6 Show Place
Christchurch, New Zealand

IT Guideline - Wireless

Southern Response Earthquake Services Limited

Author: [redacted] (IT Manager)

Document control

Change Description	Author	Version	Date	Approved By
Initial Draft	Gen-i	Draft 0.1		
Draft	[redacted]	Draft 0.2	21-04-2013	
Review	[redacted]	Draft 0.3	27-05-2014	
Review	[redacted]	Draft 0.4	8-05-2015	

Table of Contents

1) Introduction

1.1) Statement of Intent

The purpose of this document is to limit and restrict the number of wireless access points, within the organisation's premises, connecting to Southern Response's internal network or related technology resources via any means involving wireless technology.
The overriding goal of this document is to protect Southern Response's technology-based resources (such as corporate 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 Southern Response's public image. Therefore, all users employing wireless methods of accessing corporate technology resources must adhere to company-defined processes for doing so, using company-approved access points.

1.2) Scope

This document applies to all Southern Response employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize mobile computers to access the organisation's data and networks via wireless means. Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment at Southern Response does not automatically guarantee the granting of wireless access privileges. This policy is complementary to any previously implemented policies or documents dealing specifically with network access and remote access to the enterprise network.

1.3) Review

This document will be reviewed on an annual basis by the IT MANAGER. The review will assess both the content of the document and the compliance with controls identified within the document

1.4) Relevant References and Resources

- Use of Information Resources and Security Policy
- IT Standard – Acceptable Use

2) Guidelines

2.1) Access Points

Southern Response is committed to providing authorized users with wireless access to the Internet, Southern Response networks and systems, as well as other corporate resources. In order to make this convenient service available to end users, the IT Department must install "access points" in and around the premises wherever wireless access to company 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. PDA, 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 Southern Response, 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 corporate firewall will be centrally managed by Southern Response's IT Department or designated service provider and will utilize encryption, strong authentication, and other security methods at IT's discretion. Addition of new wireless access points within corporate facilities will be managed at the sole discretion of IT. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organisational premises, is strictly forbidden

2.2) Restrictions

- Southern Response uses the 802.11 protocol as its wireless network standard, transmitting at 2.4 GHz or 5 GHz radio frequency spectrum, with the intention of delivering wireless access to mobile and wireless devices
- Southern Response's IT Department will support only the following devices and equipment for accessing corporate networks and systems wirelessly:
  - Aruba IAP-130 Series Instant Access Point
  - Cisco Access Point (by exception)
- The IT Department will strive to purchase only those access points and equipment that possess the following characteristics and/or features:
  - In-built firewall
  - RADIUS authentication
  - SNMP
  - Syslog
  - WPA2 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

- All wireless clients and devices should be equipped with a host-based personal firewall and anti-virus software. The service provider shall update these applications as required, and will not reconfigure them in any way
- Whenever necessary, the IT Department or designated Service Provider 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

- All wireless access points, including those designated for networking home offices or satellite offices with the corporate network, must be approved by Southern Response's IT & Data Manager
- 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
- Use of the wireless network is subject to the same guidelines as Southern Response's technology and Internet acceptable use documents
- It is the responsibility of Southern Response employees, contractors, vendors and agents with wireless access privileges to Southern Response's corporate network to ensure that their wireless access connection is given the same consideration as the user's on-site connection to Southern Response i.e the policies applicable to wired connections are equally applicable to wireless connections and name the policies here
- Maintain a hardware address that can be registered and tracked, i.e., a MAC address
- Provide guidance in the policy to users as to what the correct procedures are for requesting a wireless access point being set-up
- All data that traverses the corporate wireless network must be encrypted, using Wi-Fi Protected Access 2 (WPA2) at minimum. The IT Department will strive to procure only WLAN equipment that supports WPA2, and will also provide suitable software for authentication and encryption.
- Southern Response's IT Department cannot guarantee 99.999 percent availability of the wireless network, especially during inclement weather. Nevertheless, the IT Department will make all possible network adjustments within the supported radio frequency spectrum
- The IT Department will conduct periodic 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
- The IT Department reserves the right to turn off without notice any access point connected to the network that it feels puts the company's systems, data, users, and clients at risk
- The wireless access user agrees to immediately report to his/her manager and Southern Response's IT Department any incident or suspected incidents of unauthorized access point installation and/or disclosure of company resources, databases, networks, and any other related components of the organisation's technology infrastructure
- Any questions relating to this document, as well as any help desk inquiries, should be directed to the IT Manager, at x7556 or email to [redacted]@southernresponse.co.nz.

3) Guideline Breach

Failure to conform to this guideline may constitute misconduct. Persistent breaches of these guidelines may constitute serious misconduct. The procedure for dealing with cases of misconduct, as outlined in the SRES's Code of Conduct, would be followed in such cases. Depending on the extent of any breach, the conduct of the employee/s concerned, the extent of material sent/received, a breach of these guidelines could result in serious consequences such as summary dismissal. It is therefore important that you read and understand these guidelines and policies.