

## Wireless Security Policy

### 1 Purpose

This policy establishes standards that must be met when wireless communications equipment is connected to <Company Name> networks. The policy prohibits access to <Company Name> networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Information Security are approved for connectivity to <Company Name>'s networks.

### 2 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of <Company Name>'s internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to <Company Name>'s networks do not fall under the purview of this policy.

### 3 Policy

#### 3.1 Approved equipment

3.1.1 All wireless LAN access must use corporate-approved vendor products and security configurations.

#### 3.2 Monitoring of uncontrolled wireless devices

3.2.1 All company locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect, classify, and disrupt communication with unapproved wireless access points.

3.2.2 All company locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect the presence of wireless devices forming a connection between the network and any wireless network. This would include laptops that are serving as a bridge between wired and wireless networks.

3.2.3 In company locations where wireless LAN access has been deployed, wireless intrusion detection systems will also be deployed to monitor for attacks against the wireless network. The wireless intrusion detection

system shall be integrated with the wireless LAN access system whenever possible.

### **3.3 Authentication of wireless clients**

- 3.3.1 All access to wireless networks must be authenticated.
- 3.3.2 The Company's existing strong password policy must be followed for access to wireless networks.
- 3.3.3 The strongest form of wireless authentication permitted by the client device must be used. For the majority of devices and operating systems, WPA or WPA2 with 802.1x/EAP-PEAP must be used. WPA2 is preferred wherever possible.
- 3.3.4 Where 802.1x authentication is used, mutual authentication must be performed. Client devices must validate that digital certificates presented by the authentication server are trusted and valid. Under no circumstances may clients disable validation of server certificates and blindly trust any certificate presented. EAP methods that do not support certificate-based mutual authentication may not be used.
- 3.3.5 EAP methods that exchange authentication credentials outside of encrypted tunnels may not be used. These methods include EAP-MD5 and LEAP.
- 3.3.6 When legacy devices that do not support WPA or WPA2 must be used on a wireless network, they will be isolated from all other wireless devices and will be restricted to the minimum required network access. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.
- 3.3.7 Any Company user with an account in a Company user database shall be able to authenticate at any Company location where wireless access is present.

### **3.4 Encryption**

- 3.4.1 All wireless communication between Company devices and Company networks must be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement.
- 3.4.2 The strongest form of wireless encryption permitted by the client device must be used. For the majority of devices and operating systems, WPA using TKIP encryption or WPA2 using AES-CCM encryption must be used. WPA2 with AES-CCM is preferred wherever possible.
- 3.4.3 Client devices that do not support WPA or WPA2 should be secured using VPN technology such as IPSEC where allowed by the client device.

- 3.4.4 The use of WEP requires a waiver from Information Security. Client devices that require the use of WEP must be isolated from all other wireless devices and will be restricted to the minimum required network access. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network

### **3.5 Access control policies**

- 3.5.1 Access to corporate network resources through wireless networks should be restricted based on the business role of the user. Unnecessary protocols should be blocked, as should access to portions of the network with which the user has no need to communicate.
- 3.5.2 Access control enforcement shall be based on the user's authenticated identity, rather than a generic IP address block. This is also known as "identity-based security."
- 3.5.3 The access control system must be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.
- 3.5.4 Access control rules must use stateful packet inspection as the underlying technology.

### **3.6 Remote wireless access**

- 3.6.1 Telecommuting employees working from remote locations must be provided with the same wireless standards supported in corporate offices.
- 3.6.2 Employees should be discouraged from connecting Company computers though consumer type wireless equipment while at home in lieu of Company-provided equipment.

### **3.7 Client security standards**

- 3.7.1 Where supported by the client operating system, the wireless network will perform checks for minimum client security standards (client integrity checking) before granting access to the Company network. Specifically:
  - 3.7.1.1. All wireless clients must run Company approved anti-virus software that has been updated and maintained in accordance with the Company's anti-virus software policy.
  - 3.7.1.2. All wireless clients must run host-based firewall software in accordance with the Company's host security policy.
  - 3.7.1.3. All wireless clients must have security-related operating system patches applied that have been deemed "critical" in accordance with the Company's host security policy.

3.7.2 Clients not conforming with minimum security standards will be placed into a quarantine condition and automatically remediated.

3.7.3 Client operating systems that do not support client integrity checking will be given restricted access to the network according to business requirements.

### **3.8 Wireless guest access**

3.8.1 Wireless guest access will be available at all facilities where wireless access has been deployed.

3.8.2 All wireless guest access will be authenticated through a web-based authentication system.

3.8.3 A single username/password combination will be assigned for all guest access. The password for guest access will be changed monthly and distributed to local facility managers.

3.8.4 Wireless guest access is available from the hours of 7:00 until 20:00 local time.

3.8.5 Wireless guest access is bandwidth limited to 2Mb/s per user.

3.8.6 Guest access will be restricted to the following network protocols:

- HTTP (TCP port 80)
- HTTPS (TCP port 443)
- POP3 (TCP port 110)
- IKE (UDP port 500)
- IPSEC ESP (IP protocol 50)
- PPTP (TCP port 1723)
- GRE (IP protocol 47)
- DHCP (UDP ports 67-68)
- DNS (UDP port 53)
- ICMP (IP protocol 1)

## **4 Definitions**

<b>Terms</b>	<b>Definitions</b>
802.11	A set of Wireless LAN/WLAN standards developed by the IEEE LAN/MAN standards committee (IEEE 802). Also commonly referred to as "Wi-Fi."
802.11i	An amendment to the IEEE 802.11 standard specifying security mechanisms for wireless networks.
802.1x	A framework for link-layer authentication specified by the IEEE.
AES-CCM	Advanced Encryption Standard-Counter with

	CBC-MAC. A wireless encryption protocol specified by IEEE 802.11i. Currently regarded as the strongest form of wireless encryption.
EAP	Extensible Authentication Protocol. A series of authentication methods used inside 802.1x to achieve wireless authentication.
IEEE	Institute of Electrical and Electronics Engineers. An international professional organization dedicated to the advancement of technology related to electricity. The IEEE is one of the main standards bodies associated with networking technology.
IETF	Internet Engineering Task Force. Develops and promotes Internet standards, in particular those of the TCP/IP protocol suite.
IPSEC	IP Security. An IETF standard for protecting IP communication by encrypting or authenticating all packets.
LEAP	Lightweight Extensible Authentication Protocol. A proprietary protocol supported by Cisco Systems that acts as an EAP method within 802.1x. LEAP was proven insecure in 2003 and does not comply with current security standards.
PEAP	Protected Extensible Authentication Protocol. A tunneled EAP method that uses a server-side digital certificate for server authentication and a username/password for client authentication.
Stateful Packet Inspection	A filtering or firewall technology that keeps track of the state of network connections, such as TCP streams, traveling across it. Only packets which match a known connection state will be allowed, while others are rejected.
VPN	Virtual Private Network. A method of building private networks on top of public networks such that the private network is protected and separate.
WEP	Wired Equivalent Privacy. This is the encryption protocol specified in the original version of IEEE 802.11. It is now deprecated and does not meet current security standards.
Wi-Fi	A set of product compatibility standards for wireless LANs based on IEEE 802.11. The Wi-Fi term is managed by the Wi-Fi Alliance. Products carrying Wi-Fi certification have passed a series of compatibility tests.

WLAN/Wireless LAN	A type of wireless system based on the IEEE 802.11 series of protocols.
WPA	Wi-Fi Protected Access. WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards. Products displaying the WPA logo have passed a certification program run by the Wi-Fi Alliance.
WPA2	Wi-Fi Protected Access version 2. WPA2 implements the full IEEE 802.11i standard, but will not work with some older network cards. Products displaying the WPA2 logo have passed a certification program run by the Wi-Fi Alliance.

© 2006 Aruba Wireless Networks, Inc. All rights reserved.