Wireless Access Point Security Guidelines (Ver. 1.0)

Network Evaluation

Tutorials and Guides to help enhance the integrity and security of your systems

Introduction

The purpose of this document is to provide guidelines for the secure deployment of Wireless Access Points (WAP). It is worth mentioning that some of the requirements and suggestions for increasing security may not be possible for existing older equipment, or for newer equipment of a highly specialized nature. Some of this equipment and its accompanying applications may have to be "grandfathered in".

These guidelines are focused on the configuration parameters for WAPs, end stations, network configurations and restrictions in particular and do not directly address any portion of application level security.

The principles of "Defense in Depth" are used here. By this, we mean that while any one tactic used to protect the network may not provide complete protection, by adding many layers of differing types of protection, we can provide a higher level of confidence for the security of the network by making it more difficult for the overall system to be compromised.

Specific recommendations are all expressed in *italics* to provide easier identification, and are repeated without accompanying text in the summary at the end.

A recommendation prefaced with an "R" is a requirement (where applicable) unless it is suffixes with an "E". Then it is an enhancement, indicating additional security, but not absolutely required.

Scope

This document addresses physical considerations, radio configurations, channel assignments, security identifiers, network names, address limitations and other schemes to reduce the risk and opportunity of unintended (i.e. unauthorized) participation in local wireless networks.

General Considerations

1. Planning for Maintenance and Upgrade

R-1.1 Check with your equipment vendor on a regular basis (Quarterly is suggested) for updates, since many newer features are being released which will aid in enhancing

overall security. Many of these new features will be applicable to equipment already in the field (e.g. firmware upgrades), thus allowing security enhancements without having to deploy new equipment.

R-1.2 Administrators should stay current on vulnerabilities, fixes and new features that relate to wireless security. Many vendors have mailing lists which will provide automatic notification of fixes, upgrades and such.

R-1.3 All periodic events (audits, checks, etc.) should be formally scheduled through a calendaring application with all appropriate personnel. Microsoft Outlook is one example. When these events are not formally scheduled, there is a tendency to skip them.

2. Securing the Management Interface

R-2.1 Choose one or two methods of access and disable the rest, particularly HTTP. The WAP itself is usually capable of being managed by one or more methods. These are often a web interface, telnet interface, SNMP management, proprietary application or serial console connection. Not all wireless devices allow for disabling of management interfaces. In those cases password management is of paramount importance.

R-2.2 If possible and workable, management interfaces should be disabled and management tasks performed through a direct serial connection should be used, and all other network accessed services disabled.

R-2.3 If management must be performed over the network, make sure that the access point cannot be managed from the wireless side. HTTP management should not be used, particularly from the wireless side..

R-2.4 If management and configuration must be performed over the network, all management traffic should be encrypted where possible. SSH and HTTPS are preferred to their unencrypted counterparts Telnet and HTTP.

R-2.5 Where practical, use access control mechanisms (firewalls, ACL's etc.) to limit the stations allowed to access the management interface of the access point. If not possible, log all traffic (see R-14.4)

R-2.6 *The default administrator name (if possible) and password should be removed or changed as soon as possible.* Keep the name and password *different* from those used on the production network to minimize the chance of compromise. This rule is specific to the administration of the wireless devices, not general network ID's.

R-2.7 Do not allow general access to the administrative interfaces on any wireless device. Many users are knowledgeable enough to make changes that enhance their own convenience while limiting the quality of security for the network as a whole.

3. Planning for Audits and Reconciliation

The primary difference between audits and reconciliation is that audits are conducted by an outside agency (even if within the company) to identify vulnerabilities, errors and oversights, whereas reconciliation is performed by the normal administrative group itself as a sanity check on their own processes.

R-3.1 A copy of the WAP system configuration should be saved to a separate non-wireless server under good access control, and updated whenever the WAP configuration is changed. If possible, a permanent read-only copy should be kept off-line. CD-ROM is ideal, but tapes or floppy diskettes will also suffice. Although not ideal, a printed copy of all relevant configuration data is also acceptable if stored securely.

If the WAP provides no direct mechanism for saving a copy of its configuration parameters, a copy should be kept by one of the following methods:

- Hand printed records
- Saved log from a telnet/ssh/serial connection
- Screen shots of GUI configuration data printed or stored on CD-R

R-3.2 At least once a year, a current copy of the WAP configuration should be compared to the stored version to make sure that there are no discrepancies. In most cases, discrepancies will turn out to be missed updates to the stored copy, in which case the new version should be stored. If there is a security related discrepancy, this should be investigated.

4. Logging

R-4.1 Events of interest (for both security and non-security related topics) on the WAP should be logged and monitored. Acceptable mechanisms to send the logging information to a server are: syslog, SNMP Traps, TFTP, and Secure Syslog. Of the four, only syslog, TFTP and SNMP traps are currently available on commercial platforms. Secure Syslog is an ongoing project in development at UCSD. It is mentioned as a point to request of vendors for improved logging.

The events logged should include at least the following:

- WLAN Requests for ANY when complex SSIDs are in use
- Use of invalid SSIDs
- Floods of 802.11 “Disassociate Management” frames (Possible DOS attack)
- Floods of 802.1x EAP failures (Possible DOS attack)
- Admin logon successes and failures
- Access point configuration changes
- Attempts to connect to access point management systems from all systems.
- All Wireless authentication attempts, both successful and unsuccessful

R-4.2 All wireless access points must log to a common, central server. This will enable administrators to more easily spot patterns of abuse or attempted abuse.

R-4.3 All logs must be reviewed on a regular basis. There are software packages on the market which can help to automate this process, but it still needs to be performed on a

regular basis (weekly to monthly), with or without automation. With automation, monitoring can be real-time if there is an alert mechanism available.

R-4.4 All logs should be retained for at least 30 days. This includes not only security events, but other events such as reboots, radio operation, hardware diagnostics and possible other events of interest.

R-4.5 All security logs should be retained for 30 days on line, and then archived to Read-Only media such as CD-R, and then retained for at least 1 year. Security logs consist of all wireless logon attempts, all administrative activities, and all receipt of invalid Ids of any sort.

Environmental Considerations

5. Physical Security for Wireless Equipment
Physical security is important here to protect the company's wireless-based assets from theft, configuration change, and compromise. This includes the possibility of unauthorized wireless access points being installed without company knowledge or permission, as well as an already approved device being used for unintended and unauthorized purposes.

R-5.1 All equipment must be secured where it cannot be tampered with. At a minimum this means locked closets or cabinets, but this could also include badge readers and video surveillance if the equipment can share facilities with other equipment.

R-5.2 Wireless enabled equipment must be physically secured when not in use. This means either locked in a closet, cabinet or other facility, or (as with some laptops) physically secured with a locking cable to prevent being taken.

R-5.3 If any wireless enabled equipment is stolen or missing, this must be reported to facilities or network security as appropriate. This will allow any special privileges granted to this equipment to be revoked immediately.

R-5.4E Facilities and Security staff should be trained to recognize wireless network access devices and report the presence of any they do not recognize to the network and/or network security groups. New installations may be reported unnecessarily, but this will serve both to verify alertness on the part of the staff, and that proper precautions and procedures are being followed.

6. Electrical and Environmental Concerns
Power spikes, surges, fluctuations, brownouts and "noise" can all cause problems with electronic equipment ranging from reboots, to actual damage to hardware. Long term exposure to high temperatures will noticeably shorten the life of electronic equipment.

R-6.1 All equipment used must be connected to commercial power through a good quality surge protector.
R-6.2E It is preferable that a UPS (Uninterruptible Power Supply) be used which has at least a 15 minute capacity under full load
.
R-6.3 All locations for electronic equipment must be kept below 80º F.

R-6.4 Per National Electrical Code, all circuits run under constant load (must have a full-time load of no more than 80% of the rated circuit breaker capacity.

Network Access Considerations

7. Network Address Management
Many WAP systems offer DHCP server service as part of their configuration. This can be configured in such a way as to limit exposure of the network. Additionally, some systems require that DHCP service be enabled in order to also activate NAT (Network Address Translation).

R-7.1 Use of NAT is recommended so that the wireless portion of the network can use private IP address space. This way, if someone does "sniff" the wireless traffic, they will not get the effective wired LAN address of the wireless device.

R-7.2 In the DHCP configuration areas, allocate only those addresses, or the range of addresses required for the number of devices planned, or planned to be active at any given time. This will minimize the opportunity for a rogue device to be granted an IP address on the wireless LAN. Some DHCP servers have the capability to reserve IP addresses for individual MAC addresses (Similar to the older BOOTP standard). This should also be used to prevent rogue devices from getting an IP address when the range of addresses (above) is tied to specific values.

R-7.3 MAC (Media Access Control) filtering should be used to keep rogue devices from gaining access to the network. While MAC addresses can be forged, this still provides an additional layer of protection.

R-7.4 Traffic from Wireless LANS should be logged and monitored for signs of hostile activity. Intrusion detection systems and firewall log monitoring and analysis are methods of accomplishing this. Although similar to Section 4 (above) this relates to monitoring ongoing traffic with real-time response with a NIDS or Firewall log monitoring system.

8. Simple Network Management Protocol (SNMP)

R-8.1 SNMP can be useful in monitoring network equipment status. Do NOT permit it to be used to manage any wireless devices. Most SNMP implementations are insecure and require minimal authentication and authorization.

R-8.2 Delete all default SNMP strings (such as PUBLIC or PRIVATE), and substitute strings constructed in the same way as strong passwords. This should be done whether or not SNMP is intended to be used, since it may get re-enabled by mistake, or some minimal functionality may remain even when disabled.

R-8.3 If SNMP is to be used, it should be used for monitoring only. Never use SNMP to actively manage a Wireless Access Point. Any SNMP functionality not required must be disabled.

R-8.4 Regardless of the application of SNMP, all wireless access points must use community strings which are different from the rest of the organizations as well as from each other. An entire organization could be compromised if the community strings were detected. This is particularly important if Read-Write SNMP strings are used.

R-8.5 If possible, and SNMP is required, all SNMP traffic should be both authenticated and encrypted. SNMP version 3 using both authentication and privacy meets this need. If this is not possible, any security enhancements available should still be used. This includes: SNMP V. 3 with either authentication or encryption, or any of the SNMP version 2 authenticated methods.

R-8.6 SNMP managed systems must be configured to accept commands and requests only from designated, wired systems, specified by IP Address.

Radio Considerations

9. Radio Access (Physical) Protocols

Wireless Access Point devices address multiple types of radio access. Some devices allow for more than one type of radio access. Some examples of these protocols or types are:

- 802.11b General Access
- 802.11b Point-To-Point Bridge
- 802.11a
- 802.11g (upcoming)
- WLI Forum OpenAir
- S-UHF
- 902 MHz

R-9.1 Configure the Wireless Access Point to accept ONLY the one type (or types) of radio equipment specifically required. This way, if a rogue radio is attached to a WAP that allows for multiple types, it will not be enabled by default.

R-9.2 Antennas should be positioned as close to the center of the facility as possible or specialized antennas used which focus most of the signal strength in "safe" directions. This reduces their range outside the building by keeping the strongest signal range within the physical boundaries of the building.

R-9.3E If the WAP is located in a metal building (many warehouses fit this definition), the frame and metal siding should be grounded to reduce (attenuate) the radio signal outside of the building. If wireless devices must be used, and security is paramount, consider enclosing the working area in a Faraday cage.

Many devices run on different frequencies or channels within their respective bands. It is recommended to do a "search" with a wireless equipped laptop in the area (up to ¼ mile) using NetStumbler or other software searching in the frequency band planned for use by the new device(s).

R-9.4 *If any are found, make sure that the specific channels or frequencies (local law permitting) are set as far away as possible to avoid interference or accidental access.*

10. Security Identifiers

Security Identifiers go by a variety of names. The purpose is the same: To make sure that only those systems with the proper name (password) are allowed to make use of the WAP. They may be called "Network Name", "SSID", "Security ID", or another name.

R-10.1 The ability to allow ANY or NULL identifiers must be disabled. Additionally many WAPs can be set to allow ANY or NULL as an identifier, which allows almost anyone to make use of the access point.

Different technologies allow for different lengths and complexities of identifiers. Some examples are:

- 802.11b – Case-sensitive, 0-32 alphanumeric characters
- 802.11a – Case-sensitive, 0-32 alphanumeric characters
- WLI OpenAir – 0-20 characters. The use of some devices effectively limit this to 16 characters
- LAN ID – Not meant as a security ID, this is meant for control of bridging networks, but aids in preventing accidental access to a LAN. Normally used only with Spanning Tree (bridged) networks.

R-10.2 Network names and/or security identifiers should be composed of cryptic strings. They should NOT be easy-to-read strings such as "manufacturing" or "accounting23".

R-10.3 Default manufacturer strings must be replaced, as these values are sent in clear text.

Since these identifiers do not need to be entered on a regular basis by humans, this should not be a problem. Some examples are:

- `Skty45Mmzp1BeeL0` (16 characters)
- `B7aqP3U8e610popoRsmnb34wKKlp04c4` (32 characters)
- `SKWQOPRKCCKWUFMV` (16 characters ALPHA only)
- `JCVNVCODHGMBVODMNCBS` (20 characters, ALPHA only)

11. Wired Equivalent Privacy (WEP)
The purpose of Wired Equivalent Privacy is to add encryption to all wireless transactions so that a third party with a wireless "sniffer" cannot read transactions occurring over the wireless network.

R-11.1 *While the encryption for WEP has long since been broken, due to flaws in design and implementation, it is still necessary to use it since it adds some layer of difficulty for any attempted compromise and eliminates some clear-text information gathering.*

R-11.2 Dynamically generated, automatically changed WEP keys (rapid WEP re-keying) should be used where possible. The keys should be re-generated on a regular basis – typically every few seconds or minutes at most. This will necessitate the use of 802.1x services which are also used for user/node authentication.

Static WEP keys are discouraged unless there is no alternative due to the devices in use. Some older or specialized equipment may not have the capability, in which case strict ACL's are required.

R-11.3 *If the use of static WEP keys is necessary, use WEP-128 if possible, and obtain new keys. Never use default static keys.*

R-11.4 Broadcasts should be disabled whenever possible to avoid sending information unnecessarily. Some vendors provide the ability to turn off broadcast responses. As a side benefit, some vendor's implementations of this also extend battery life by not "waking up" devices not in use.

12. User or Node Authentication
R-12.1 User or node authentication must be performed on an individual device basis. Do not use common (group) identifiers for multiple devices. This is for access authentication and should not be confused with the security identifier (SSID).

R-12.2 Remove all vendor default logins. If this is not possible, then assign them strong passwords, and do not use these accounts unless the ability to create new accounts is restricted.

R-12.3 All WLAN access points must require user or node shared key 802.1x authentication wherever possible. This step often requires the presence of a RADIUS server on the wired network. Some access points incorporate a RADIUS server. Unless the users are unique to that access point, a network based RADIUS server is recommended. User devices must have supplicant capability to make use of this form of authentication.

R-12.4 802.1x re-authentication must be performed at least every 30 minutes. This is necessary for WEP re-keying and also helps keep the state between the 802.1x sessions

and the 802.11 client associations synchronized. This should be transparent to the end user, since this information is cached on the end station.

R-12.5 Where possible, wireless end stations must reject unencrypted traffic when WEP is enabled. This helps protect end systems by preventing association with rogue or other access points that are not running WEP.

R-12.6 All accounts must have passwords (technology permitting).

R-12.7 Passwords should be changed every 30 days and this policy enforced.

R-12.8 Wireless Access passwords should be different from normal (wired) system access accounts where possible see 12.3 (RADIUS). This is to keep network server passwords from being compromised by a "sniffed" Wireless access password.

R-12.9 Passwords should not be re-used. Where possible, a password history should be kept by the authenticating system to enforce this.

R-12.10 If passwords are allowed, they should meet the "strong password" criteria. Good passwords are comprised of mixtures of three of the four sets below and the following characteristics:

- Upper case letters A-Z
- Lower case letters a-z
- Numerical values 0-9
- Special symbols *!@#$%^&*()_+-={}[]|\:;"'<>?,./*
  NOTE: Not all symbols are allowed. This will vary by vendor and model.
- Length of 8 or more characters
- No association with personal information: Names, Birthdays, license plate number, social security numbers, dates, etc.
- Mnemonics phrases can be used to make it easier to remember complex passwords. For example: The phrase "Don't quote me" could be expressed as Don't"Me which contains upper and lower case letters and symbols, and is memorable. Short phrases with substitutions of uppercase or misspellings also work, e.g. ¼#Berger would be "Quarter pound burger". Nonsense phrases or terms are even better, since there is less chance of discovery and/or compromise.

E-12.11 Optionally, automatically derived, one-time password tokens may be used. SecureID and CryptoCARD are examples of this type of technology.

13. Bridged Wireless LANs

R-13.1 IAPP Security Context Hand Off should be employed where the wireless devices roam from one wireless LAN to another in a bridged wireless network (DIVERSITY RECEPTION). This simplifies the re-authentication process between LANs. Use the same *type* of IAPP Secret key as used for other authentication; i.e. long cryptic strings with no identifiable meaning. See the password section on what constitutes a strong password.

R-13.2 Use a LAN ID (Domain) other than the default of 0 or 255 when building Spanning Tree bridged networks. NOTE: OpenAir radio equipment uses the LAN ID modulo 16, that is, the remainder after dividing the LAN ID by 16.

14. Data Confidentiality, Integrity and Application Level Security

R-14.1 All wireless traffic destined for corporate IT resources should be encrypted with a known robust protocol. SSH/SSL

R-14.2 Where possible, use encrypted protocols (HTTPS and SSH) in favor of their unencrypted counterparts for WAP management.

VPNs (Virtual Private Networks) provide an additional layer of security by requiring an authentication of their own, as well as a better form of encryption to protect the transmitted data from interception and deciphering.

R-14.3 If native encrypted protocols (HTTPS and SSH) are not appropriate or available for the applications in use, then VPNs should be used to protect the confidentiality and integrity of data passing over a WLAN.

R-14.4 All wireless traffic should be passed through a firewall or other access control systems. These should be configured to limit the types (protocols, port numbers) of traffic allowed, as well as the destination addresses, so that an intruder or rogue device is limited in areas of access. This differs from item R-2.5 which is intended to keep unauthorized users from the administrative interface of wireless equipment. The purpose of this is to mitigate harm or damage to production systems should an unauthorized user gain access through a wireless device.

15. Wireless Equipment in Public or Semi-Public sites

This section is intended to differentiate any requirements for portions of the network which may be intended for use by the public, customers, vendors or anyone else who is not an actual employee or contractor of the company. These will be collectively referred to as “outsiders” below.

R-15.1 All network addressing schemes, LAN ID’s WEP keys and user ID’s and passwords will be different from those used elsewhere on or at that site. This is to prevent any “sniffed” data from being usable against other wireless network segments.

R-15.2 All network segments accessible to outsiders will be kept separate from other network segments that connect to the rest of the company network. This may be accomplished by physical separation or by strict firewall configuration. Under no circumstances should any outsider’s equipment be allowed access to the general production network.

Summary

This section is a condensed version of the recommendations above, but without commentary or discussion. General requirements or recommendations are marked R-x.x. Suggestions for enhancements are suffixed with the letter E as in R-x.xE.

R-1.1 Check with your equipment vendor on a regular basis (Quarterly is suggested) for updates, since many newer features are being released which will aid in enhancing overall security.

R-1.2 Administrators should stay current on vulnerabilities, fixes and new features that relate to wireless security.

R-1.3 All periodic events (audits, checks, etc.) should be formally scheduled through a calendaring application with all appropriate personnel.

R-2.1 Choose one or two methods of access and disable the rest, particularly HTTP.

R-2.2 If possible and workable, management interfaces should be disabled and management tasks performed through a direct serial connection should be used, and all other network accessed services disabled.

R-2.3 If management must be performed over the network, make sure that the access point cannot be managed from the wireless side. HTTP management should not be used, particularly from the wireless side..

R-2.4 If management and configuration must be performed over the network, all management traffic should be encrypted where possible.

R-2.5 Where practical, use access control mechanisms (firewalls, ACL's etc.) to limit the stations allowed to access the management interface of the access point. If not possible, log all traffic (see R-14.4)

R-2.6 The default administrator name (if possible) and password should be removed or changed as soon as possible.

R-2.7 Do not allow general access to the administrative interfaces on any wireless device.

R-3.1 A copy of the WAP system configuration should be saved to a separate non-wireless server under good access control, and updated whenever the WAP configuration is changed.

R-3.2 At least once a year, a current copy of the WAP configuration should be compared to the stored version to make sure that there are no discrepancies

R-4.1 Events of interest (for both security and non-security related topics) on the WAP should be logged and monitored.

R-4.2 All wireless access points must log to a common, central server.

R-4.3 All logs must be reviewed on a regular basis.

R-4.4 All logs should be retained for at least 30 days.

R-4.5 All security logs (as opposed to general logs) should be retained for 30 days on line, and then archived to Read-Only media such as CD-R, and then retained for at least 1 year. Security logs consist of all wireless logon attempts, all administrative activities, and all receipt of invalid Ids of any sort.

R-5.1 All equipment must be secured where it cannot be tampered with.

R-5.2 Wireless enabled equipment must be physically secured when not in use.

R-5.3 If any wireless enabled equipment is stolen or missing, this must be reported to facilities or network security as appropriate.

R-5.4E Facilities and Security staff should be trained to recognize wireless network access devices and report the presence of any they do not recognize to the network and/or network security groups.

R-6.1 All equipment used must be connected to commercial power through a good quality surge protector.

R-6.2E It is preferable that a UPS (Uninterruptible Power Supply) be used which has at least a 15 minute capacity under full load.

R-6.3 All locations for electronic equipment must be kept below 80º F.

R-6.4 Per National Electrical Code, all circuits run under constant load must have a full-time load of no more than 80% of the rated circuit breaker capacity.

R-7.1 Use of NAT is recommended so that the wireless portion of the network can use private IP address space.

R-7.2 In the DHCP configuration areas, allocate only those addresses, or the range of addresses required for the number of devices planned, or planned to be active at any given time.

R-7.3 MAC (Media Access Control) filtering should be used to keep rogue devices from gaining access to the network.

R-7.4 Traffic from Wireless LANS should be logged and monitored for signs of hostile activity.

R-8.1 SNMP should NOT be used to manage any wireless devices.

R-8.2 Delete all default SNMP strings (such as PUBLIC or PRIVATE), and substitute strings constructed in the same way as strong passwords.

R-8.3 If SNMP is to be used, it should be used for monitoring only.

R-8.4 Regardless of the application of SNMP, all wireless access points must use community strings which are different from the rest of the organizations as well as from each other.
R-8.5 If possible, and SNMP is required, all SNMP traffic should be both authenticated and encrypted.

R-8.6 SNMP managed systems must be configured to accept commands and requests only from designated, wired systems, specified by IP Address.

R-9.1 Configure the Wireless Access Point to accept ONLY the one type (or types) of radio equipment specifically required.

R-9.2 Antennas should be positioned as close to the center of the facility as possible or specialized antennas used which focus most of the signal strength in "safe" directions.

R-9.3E If the WAP is located in a metal building (many warehouses fit this definition), the frame and metal siding should be grounded to reduce (attenuate) the radio signal outside of the building. If wireless devices must be used, and security is paramount, consider enclosing the working area in a Faraday cage.

R-9.4 If a search for adjacent wireless systems shows that any were found, make sure that the specific channels or frequencies (local law permitting) are set as far away as possible to avoid interference or accidental access.

R-10.1 The ability to allow ANY or NULL identifiers must be disabled

R-10.2 Network names and/or security identifiers should be composed of cryptic strings. They should NOT be easy-to-read strings such as "manufacturing" or "accounting23".

R-10.3 Default manufacturer strings must be replaced, as these values are sent in clear text.

R-11.1 While the encryption for WEP has long since been broken, due to flaws in design and implementation, it is still necessary to use it since it adds some layer of difficulty for any attempted compromise and eliminates some clear-text information gathering.

R-11.2 Dynamically generated, automatically changed WEP keys (rapid WEP re-keying) should be used where possible. The keys should be re-generated on a regular basis – typically every few seconds or minutes at most.

R-11.3 If the use of static WEP keys is necessary, use WEP-128 if possible, and obtain new keys. Never use default static keys.

R-11.4 Broadcasts should be disabled whenever possible to avoid sending information unnecessarily.

R-12.1 User or node authentication must be performed on an individual device basis. Do not use common (group) identifiers for multiple devices.

R-12.2 Remove all vendor default logins. If this is not possible, then assign them strong passwords, and do not use these accounts unless the ability to create new accounts is restricted.

R-12.3 All WLAN access points must require user or node shared key 802.1x authentication wherever possible.

R-12.4 802.1x re-authentication must be performed at least every 30 minutes.

R-12.5 Where possible, wireless end stations must reject unencrypted traffic, when WEP is enabled.

R-12.6 All accounts must have passwords (technology permitting).

R-12.7 Passwords should be changed every 30 days, and this policy enforced.

R-12.8 Wireless Access passwords should be different from normal (wired) system access accounts where possible see 12.3 (RADIUS).

R-12.9 Passwords should not be re-used.

R-12.10 If passwords are allowed, they should meet the "strong password" criteria.

E-12.11 Optionally, automatically derived, one-time password tokens may be used.

R-13.1 IAPP Security Context Hand Off should be employed where the wireless devices roam from one wireless LAN to another in a bridged wireless network (DIVERSITY RECEPTION).

R-13.2 Use a LAN ID (Domain) other than the default of 0 or 255 when building Spanning Tree bridged networks.

R-14.1 All wireless traffic destined for corporate IT resources should be encrypted with a known robust protocol.

R-14.2 Where possible, use encrypted protocols (HTTPS and SSH) in favor of their unencrypted counterparts for WAP management.

R-14.3 If native encrypted protocols (HTTPS and SSH) are not appropriate or available for the applications in use, then VPNs should be used to protect the confidentiality and integrity of data passing over a WLAN.

R-14.4 All wireless traffic should be passed through a firewall or other access control systems.

R-15.1 All network addressing schemes, LAN ID's WEP keys and user ID's and passwords will be different from those used elsewhere on or at that site.

R-15.2 All network segments accessible to outsiders will be kept separate from other network segments that connect to the rest of the company network.