Corporate Compliance Information Security Department Policy & Procedure	
Subject	**802.11 Protocol Family of Wireless Networks**
Reference Standards	**ISO 17799, NIST SP800-48 Wireless Network Security**
Policy #	**<POLICY CODE>**
Effective Date	**<EFFECTIVE DATE>**

PURPOSE

As wireless technology is increasing in popularity, driven by productivity gains and convenience, it also presents new security challenges, especially as they relate to confidentiality and integrity of data. Wireless technology enables flexible connection to the corporate network, but connecting through a wireless device can often bypass existing wired-side security measure.

POLICY:

Access to <COMPANY> data or applications via ***unsecured*** 802.11 family wireless devices, networks or technologies is prohibited. Only 802.11 family wireless devices, networks, or technologies that meet the criteria of this policy or have been granted a waiver by the Corporate Compliance Information Security Officer and Information Systems are approved for connectivity to <COMPANY>'s networks. Ad-hoc or peer-to-peer wireless communication is not allowed.

This policy will establish and document standards for how the 802.11 protocol family of wireless devices, networks, and technologies will be securely implemented throughout <COMPANY>.

This policy applies to all employees, visitors and contractors. Policy enforcement is critical to ensure secure operation of the wireless network and prevent intrusions. When this policy is violated, the individual that violates the policy directives will be immediately notified, and appropriate legal and professional action will be taken against that individual.

Corporate Compliance Information Security Officer	<NAME OF AUTHORITY FOR THIS POLICY>	<CONTACT INFO>
Executive Sponsor	<NAME>	<CONTACT INFO>
Emergency Response Team	<NAME>	<CONTACT INFO>
	<NAME>	<CONTACT INFO>
	<NAME>	<CONTACT INFO>
	<NAME>	<CONTACT INFO>
	<NAME>	<CONTACT INFO>

RISK ASSESSMENT

Security Audit

A risk assessment of each WLAN will be done by Information Systems. The risk assessment should include identification of data sensitivity, network vulnerabilities, critical services, and personnel deficiencies. Security measures commensurate with the risks and threats associated

with the WLAN should be implemented. Risk assessments should be performed periodically and at least every 12 months.

Threat Prevention
A Wireless LAN Intrusion Detection System should be deployed to perform dedicated monitoring of the airwaves. The architecture should be able to provide an enterprise view of the WLAN being monitored at a glance with the ability to analyze any specific area/section of the WLAN. The wireless Intrusion Detection System should be able to detect and alert on wireless intrusion activities, including but not limited to:

- Rogue Access Points and any rogue 802.11 devices
- Accidental, Ad-hoc and Malicious Associations
- Probing Stations
- Ad-hoc networks and other device misconfigurations
- Unauthorized Network Access
- MAC spoofing
- Denial of Service (DoS) Attacks
- Identity Theft
- Malicious Data Insertion
- 802.11 Protocol misuse

FUNCTIONAL POLICY – GUIDELINES & BASELINE PRACTICES

Acceptable Use
Access to <COMPANY> data or applications via **unsecured** 802.11 family wireless devices, networks or technologies is prohibited. Only 802.11 family wireless devices, networks, or technologies that meet the criteria of this policy or have been granted a waiver by the Corporate Compliance Information Security Officer and Information Systems are approved for connectivity to <COMPANY>'s networks. Ad-hoc or peer-to-peer wireless communication is not allowed.

Corporate Compliance Information Security responsibilities:

1. Evaluating the security of all 802.11 family devices, networks, and technologies
2. Setting the standards all 802.11 family devices, networks, and technologies must meet to be allowed for use within <COMPANY>
3. Creating and maintaining privacy and security policies and procedures regarding the use of 802.11 family devices, networks, and technologies within <COMPANY>
4. Periodically auditing the 802.11 networks for security issues and resolving any issues found
5. Oversight review of risk assessments at least every 12 months.

Information Systems responsibilities:

1. Approving the use of all 802.11 family devices, networks, and technologies ***prior*** to their installation and implementation.
2. Creating and maintaining a list of wireless devices approved for use with the 802.11 family of networks and technologies within <COMPANY>.
3. Setting up, configuring, monitoring, backup, and maintaining <COMPANY> owned 802.11 family access points, switches, client devices, and any anything else related to the 802.11 wireless networks.
4. Following the procedure section of this document when setting up and configuring 802.11 devices, networks, and technologies.
5. Changing the manual WEP keys and Administrative passwords and notifying the Corporate Compliance Information Security Officer of the change.

6. Daily real-time monitoring of the 802.11 networks for performance and security issues, resolving, documenting, and reporting any issues or findings.
7. Monthly summation report of daily monitoring findings to the Corporate Compliance Information Security Officer.
8. Quarterly check the satellite facilities for rogue devices and availability.
9. Monthly availability testing in all main facilities.
10. Perform and document risk assessments at least every 12 months. Results of assessment must be submitted to the Corporate Compliance Information Security Officer within 30 days. Documentation must contain plan of corrective action if applicable.
11. Manage all devices in compliance with <COMPANY> asset management policies and procedures.
12. Coordinate external service for end device to ensure the protection of <COMPANY> data in compliance with <COMPANY> information protection and destruction guidelines and policies.
13. Prior to destruction or abandonment of a wireless end device the customer will submit the device to <COMPANY> IS for the destruction/removal of any/all <COMPANY> information from the device in compliance with <COMPANY> policy and guidelines or surrender the device to <COMPANY> for destruction.
14. Maintain documentation of all device (end and infrastructure) life histories. Annual provide copies of documentation to the Corporate Compliance Information Security Officer.

End Device Customer Responsibilities:

1. Customer using the device must comply with all <COMPANY> security guidelines and policies.
2. Customer must not disable of modify the device without permission of the <COMPANY> CIO and the Corporate Compliance Information Security Officer.
3. Customer must maintain possession of and protect the wireless end device in compliance with <COMPANY> guidelines and policies.
4. Customer must immediately report to <COMPANY> any loss or breech (suspected or observed) of the wireless end device.
5. Customer will only connect the end device to a <COMPANY> managed network.
6. Customer will coordinate service (maintenance, repair, etc.) of the end device with <COMPANY> IS to ensure the protection of any <COMPANY> information stored on the device.
7. Prior to destruction or abandonment of the wireless end device the customer must submit the device to <COMPANY> IS for the destruction/removal of any/all <COMPANY> information from the device in compliance with <COMPANY> policy and guidelines or surrender the device to <COMPANY> for destruction.

FUNCTIONAL POLICY – DESIGN & IMPLEMENTATION

Preferred wireless protocol

802.11i is the preferred wireless network protocol for <COMPANY>. 802.11 family wireless devices or networks running anything other than 802.11i will have restrictions imposed based on application necessity and deployment. 802.11 family wireless devices or networks running 802.11i will have full access to <COMPANY> information system assets.

Encryption of confidential data

Encryption will be used to protect wireless transmissions of confidential data. At a minimum, 128 bit WEP will be implemented on any wireless network that carries confidential data. A

better encryption method will be to use WPA. The best encryption solution will be to use 802.11i. A VPN may also be used to protect wireless transmissions.

Public Wireless Network
There can be one public wireless network at each location. Guests will be allowed to use this network. No <COMPANY> data or applications will be allowed on this network. All authentications to the Internet for the public network will be handled by proxy.

<COMPANY> owned client devices
<COMPANY> owned client devices will be configured by Information Systems, or their designee, with the wireless networks the client device is allowed to access. Client devices will be configured to only connect to the preconfigured networks. No other wireless networks are allowed on the <COMPANY> provided client device. Current antivirus and firewall software will also be installed and configured on the device by Information Systems.

Standard configuration settings
The following standard configuration settings should be used on all wireless equipment as appropriate for each piece of equipment:

1. The broadcast SSID feature will be disabled (except on the public network)
2. All default settings should be changed (passwords, SSIDs, channels, etc.)
3. All unnecessary services will be removed
4. Logging will be enabled
5. The SSIDs and passwords will be complex
6. SSIDs will not reflect the name of the organization, department, location, etc.
7. All security features of the equipment will be enabled.

Network segregation
The wireless network will be segregated from the wired network so a security breach on a wireless segment will not as easily affect the wired network. A firewall will be placed between the wired and wireless networks to control and monitor the traffic between them.

Rogue access point detection
In the main facilities, strategically placed nodes will be used to continually scan for rogue access points and either disconnect the port or notify Information Systems of it. At the satellite facilities, Information Systems will manually scan for rogue devices quarterly using PDAs, laptops or some other portable device.

Availability testing
Wireless availability tests should be performed quarterly in the satellite facilities and monthly in the main facilities. 802.11 client software can be used to assess if signal strength is appropriate for an area. Coverage of the wireless network ***must not*** extend beyond the interior of the building.

Manual WEP Keys and Admin Passwords
The manual WEP keys and administrator password for each wireless network will be maintained in a password protected and encrypted file by the Information Systems Network Engineer(s). Only the Information Systems Network Engineer(s) and the Network Security Administrator will have the password to this file. The manual WEP keys will be changed whenever:

1. someone who knows them is no longer in a position to need to know them
2. anytime it is suspected they have been compromised
3. anytime the Corporate Compliance Information Security Officer requests it.

The administrator password will be changed every 90 days or whenever:

1. someone who knows them is no longer in a position to need to know them
2. anytime it is suspected they have been compromised
3. anytime the Corporate Compliance Information Security Officer requests it.

Anytime a WEP key or an administrative password is given to anyone other than an Information Systems Network Engineer or Corporate Compliance Information Security, a log of what information was given to whom and when as well as why will be created and maintained by the party giving out the information. This log may be audited at any time by Corporate Compliance Information Security.

FUNCTIONAL POLICY – MONITORING & RESPONSE

Monitoring/Auditing

Activities on all wireless networks are subject to monitoring and auditing. Attempts to bypass security or to damage the system in any way, passively or actively, are strictly prohibited. The use of scanning software to capture data from the wireless network for any reason other than daily monitoring of the performance or security of the network is strictly prohibited except for personnel authorized by the Corporate Compliance Information Security Officer.

Procedures

Only Information Systems, or their designee, is permitted to setup and configure access points, switches, client devices, and anything else related to wireless networking. Information Systems, or their designee, will perform the following steps:

Access Point/Switch requirements:

1. Ensure AP/switch has flashable firmware so that security patches may be deployed as they become available.
2. Enable WEP to 128-bit
3. WEP keys will be changed anytime someone who knows them is no longer in a position to need to know them, or any time the Corporate Compliance Information Security Officer requests them to be changed.
4. Change the default SSID in the AP/switch
5. Disable the broadcast SSID feature so that the client SSID must match that of the AP/switch
6. Change the default password in the AP/switch
7. Disable all insecure and nonessential management protocols on the AP/switch. The AIMDatabase should be documented with the protocols disabled on the AP/switch.
8. Ensure the AP/switch has a strong administrative password
9. Ensure all AP/switch passwords are changed every 90 days
10. Create accounts on the AP/switch for use to configure the device by people authorized by the CIO to configure the device.
11. If practical, turn the AP/switch off when it is not in use (e.g. after hours, weekends)
12. Turn on logging in the AP/switch and review the logs weekly for suspicious or unusual activity. All unusual activity will be reported to the Corporate Information Security Officer. Logs should be retained for 6 months.
13. Password controls on the AP/switch should be set to a minimum length of 8 characters, alpha/numeric/special characters required (at least one of each), expiration date of not more than 90 days, passwords are not allowed to be reused for at least 8 periods
14. Coverage by the AP must not extend beyond the interior of the building

15. The AP must be ceiling or wall mounted away from normal reach
16. Whenever possible, the AP should be mounted out of view from casual observers
17. Switches should be mounted in locked closets
18. Only people authorized by the CIO may reset an AP
19. Make sure all default settings are changed in the AP/switch
20. Enable all security features of the AP/switch
21. When disposing of APs/switches that will no longer be used by the organization, clear the configuration to prevent disclosure of network configuration, keys, passwords, etc. through permanent information destruction methodologies in compliance with <COMPANY> information destruction guidelines and policies.
22. When surrendering a component of the wireless infrastructure for external service/support all configuration information will be cleared through permanent data destruction methodologies in compliance with <COMPANY> information destruction requirements.

SSID requirements

1. The SSID will not reflect the organization's name, department name, location, street address, or services.
2. The SSID will not contain words found in a dictionary in any language.
3. The SSID will be long and difficult to guess.
4. The SSID will be composed of mixed case letters, numbers, and special characters.

Network configuration requirements

1. Use SNMP version 3 and/or SSL/TLS for Web-based management of the AP/switch.
2. Use DHCP IP addressing only for client devices.
3. Use static IP addressing maintained by the DHCP Server for the AP.
4. Use shared-key authentication.
5. Make sure that default shared keys are replaced by more secure unique keys.
6. Deploy Radius and turn on logging. The logs should be reviewed weekly for suspicious or unusual activity. All unusual activity will be reported to the Corporate Compliance Information Security Officer. A copy of the log containing the suspicious or unusual activity will be submitted to the Corporate Compliance Information Security Officer. Logs should be retained for 6 months.
7. Fully test and deploy software patches and upgrades on a regular basis.
8. Enable user authentication mechanisms for the management interfaces of the AP/switch.
9. Ensure that management traffic destined for the AP/switch is on a dedicated wired subnet.
10. Any 802.11 protocol family wireless network must be in a DMZ behind a properly configured firewall.
11. Change the default SNMP community string to a strong community string (mixed case letters, numbers, special characters).
12. Use a local serial port interface or the wired LAN for AP configuration to minimize the exposure of sensitive management information.
13. Make sure all default settings are changed.
14. Enable all security features of the WLAN product.
15. Do not allow anything to connect at less than 11mb in the main facilities.

End Device requirements

1. Install and keep current antivirus software on all wireless clients.
2. Install and keep current personal firewall software on all wireless clients.
3. Disable file sharing on wireless clients.

4. Fully test and deploy software patches and upgrades on a regular basis.
5. Ensure the “ad hoc mode” has been disabled.
6. Ensure the client device is protected from data theft if the device is lost or stolen (e.g. use software that decrypts/encrypts the entire device upon power up/down, strong password or a biometric to authenticate authorized users).
7. End device must be managed by Information Systems in compliance with applicable <COMPANY> asset management methodologies.
8. Destroy or eradicate all <COMPANY> information from all end of life, abandoned or inoperable end devices in compliance with <COMPANY> compliance/security data destruction requirements.

Monitoring/Auditing requirements

1. Intrusion Protection will be deployed to monitor for rogue APs and rogue devices on a 24x7 basis in all main facilities. Monitoring areas will include both known and unknown wireless network areas of the main facilities.
2. The wireless Intrusion Detection System must facilitate the definition and enforcement of corporate WLAN policy.
3. Monitor for Ad-hoc associations, accidental associations, and soft APs.
4. The intrusion detection system must provide built-in mechanisms to help mitigate the risks posed by mis-configured devices, threats and other malicious activity. The active responses include but are not limited to wired-side port termination, wireless termination, on-command termination and policy termination.
5. Sniffers or other data captures are not permitted except by personnel authorized by the Corporate Compliance Information Security Officer.
6. If rogue APs are detected at the main facilities, the port will be disconnected.
7. Real time network audits to inventory all hardware used for data communications will be done on internal networks in the main facilities.
8. The digital “fingerprints” vendor-specific characteristics and personal trademarks of authorized users will be used to identify intruders on the internal networks at the main facilities.
9. Real time intrusion detection will be utilized at the main facilities. The solution must perform dedicated monitoring and provide the Enterprise view of the WLAN being monitored.
10. Intrusion Protection logs should also be reviewed weekly for suspicious or unusual activity. The system should have extensive mechanisms to perform forensic analysis on historic data. Logs should be recorded and retained for 6 months.
11. All detected suspicious activity will be documented and immediately reported to the Corporate Compliance Information Security Officer.

Public Access to Guest Wireless LAN (no <COMPANY> data on this WLAN) requirements

1. Display warning banner upon connection that must be clicked for acceptance that they are to use the public wireless access responsibly and will not attempt to intrude or damage any network, wireless or wired.

Policy Maintenance: The Corporate Compliance Information Security department is responsible for the interpretation and maintenance of this policy.

Approved by: <NAME> <DATE>

APPENDIX - DEFINITIONS

DEFINITION(S):

802.1x: A specification for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. It ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods.

802.11: refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997. There are several specifications in the 802.11 family:

> *802.11* -- applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
>
> *802.11a* -- an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
>
> *802.11b* (also referred to as WiFi) -- an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
>
> *802.11g* -- applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.
>
> *802.11i* -- incorporates 802.1x , strong encryption techniques such as AES (Advanced Encryption Standard), and EAP authentication methods to improve WLAN security.

Access Point (AP): a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect.

Ad-hoc mode: A networking framework in which devices communicate directly with each other, without the use of an access point (AP). Ad-hoc mode is also referred to as peer-to-peer networking.

Authentication: The process of identifying an individual, usually based on a username and a password. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Basic Service Set (BSS): a set of wireless devices that can communicate with each other

Client: any device a person uses to connect with a network. (i.e. laptop, PDA, tablet)

Extensible Authentication Protocol(EAP): a general protocol for authentication that also supports multiple authentication methods, such as token cards, one-time passwords, and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as Radius. The server asks the AP for proof of identity, which the AP then gets from the user and then sends back to the server to complete the authentication.

Encryption: Prevents any non-authorized party from reading or changing data. The level of protection provided by encryption is determined by an encryption algorithm. In a brute-force attack, the strength is measured by the number of possible keys and the key size. For example, a Triple-Data Encryption Standard system (3 DES) uses 112-bit or 168-bit keys. Business to Business VPNs (Extranets) share sensitive data with multiple organizations, so demand the highest level of security. This requires public key encryption and/or secure key exchange, both of which are designed to eliminate the risk of the key becoming known to an unauthorized party.

MAC Address: Short for Media Access Control Address. It is a unique hardware number that identifies each node of a network.

Information Systems Asset: <COMPANY> information, data, equipment and systems. Examples include but are not limited to: operating systems, software, applications, browsers, databases, programs, computers, servers, mobile computing devices, LAN, WAN, routers, etc.

Peer to peer: A networking framework in which devices communicate directly with each other, without the use of an access point (AP). It is also known as ad-hoc networking.

Protocol: A common set of rules and signals that computers on the network use to communicate.

Radius: Short for Remote Authentication Dial-In User Service. It is a central point of authentication for remote access that relieves a number of burdens for administrators by utilizing an existing directory of users to authenticate against.

Rogue Access Point: an authorized access point

Sniffer: A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere.

SSID: Short for service set identifier. It is a unique identifier sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another, so all access points and devices attempting to connect to a specific WLAN must use the same SSID. A device is not permitted to join the BSS unless it can provide the correct unique SSID. Because an SSID can be sniffed in plain text from a WLAN packet, it does not supply any security to the network. The SSID is also called a network name because essentially it is a name that identifies a wireless network.

WEP: Short for Wired Equivalent Privacy. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed so it provides little security to the network.

Wi-Fi: Short for wireless fidelity and is used to refer to any type of 802.11 network.

WLAN: A wireless local area network.

Workforce: Consists of employees, volunteers, contractors, consultants, trainees and other persons who perform work for <COMPANY>, (including those workers affiliated with third parties) who may have access to <COMPANY>'s Information Systems and/or equipment, regardless of whether or not compensation is received from <COMPANY>.

WPA: Short for Wi-Fi Protected Access, a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP (i.e., as a software upgrade to existing hardware), but the technology includes two improvements over WEP:

- Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
- User authentication, which is generally missing in WEP, through the EAP. WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

It should be noted that WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion.