WIRELESS SECURITY

General Overview

The use of wireless technologies has become widespread today, thanks in large part to its ease of installation, portability, along with advances in security, such as industry accepted encryption measures. Though the scope of wireless itself can be rather large, for purposes of this stated policy and supporting procedures, the focus is on the configuration, implementation, monitoring, and overall security of an organization's wireless platform used by authorized individuals, specifically, a Wireless Local Area Network (WLAN).

While wireless does indeed provide numerous benefits, insecure platforms pose significant risks, potentially leading to security breaches that can be extremely damaging, financially and operationally. Stories abound of poorly provisioned wireless platforms being compromised by malicious individuals, hackers, and other harmful individuals, ultimately compromising the confidentiality, integrity, and availability (CIA) of an organization's overall information systems landscape. Failing to remove vendor default settings, broadcasting SSID's further then required, utilizing poor encryption protocols - these are just a few of the many examples of wireless gone wrong - all the more reason for having a well-defined, comprehensive wireless security policy and procedures document in place.

The technology for securing wireless is widely available, works well and requires a dedicated effort amongst all users within an organization - but technology is only as good as the policies and procedures guiding such practices - hence, the reason for a clearly written wireless security policy. It's also important to note that end-user devices - laptops, desktops, and other workstations used for accessing wireless platforms - must be properly protected from malware and other malicious exploits. In summary, a sound wireless security policy is paramount in today's world of growing cyber security threats, and following such practices is a must for organizations seeking to protect the safety and security of critical system resources.

Wireless Security Policy and Procedures

Title	**[company name] Wireless Security Policy and Procedures**
Version	Version 1.0
Date	TBD
Language	English
Individual and/or Department Responsible for Distribution of Document	[company name] Information Technology Department
Individual and/ or Department Responsible for Timely Update of Document	[name and title]
Developed by:	[company name]
Subject	Use of Software
Approval Date	TBD
Purpose of Document	To implement comprehensive wireless security policies, procedures, and practices whereby all employees and other intended parties are readily aware of the organization's wireless security initiatives.
Distribution of Document	Disbursed to all employees of [company name] and available by request to all other intended parties.

1.0 Overview

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal Wireless Security policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 Purpose

This policy and supporting procedures are designed to provide [company name] with a documented and formalized Wireless Security policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of [company name] system resources. Advances in technology have resulted in the increased reliance on wireless platforms as they provide portability, flexibility, and are relatively inexpensive to implement. However, poorly configured Wireless Local Area Networks (WLAN) can pose significant security challenges, possibly compromising an organization's information systems landscape. The subsequent policies and procedures relating to wireless security initiatives for [company name] strive to ensure the overall confidentiality, integrity, and availability (CIA) of the organization’s network.

1.0 Scope

This policy and supporting procedures encompasses all system resources that are owned, operated, maintained, and controlled by [company name] and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.

- External system resources are those owned, operated, maintained, and controlled by any entity other than [company name], but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal system resources".

- When referencing the term “users”, this includes any individual that has been granted remote access rights by [company name] and has went through all required provisioning steps. Users typically include, but may not be limited to, the following: employees, consultants, vendors, contractors, along with local, state, and federal personnel.

1.0 Policy

[Company name] is to ensure that the Wireless Security policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Design and Configuration Analysis

[Company name] is to ensure that the deployment of any Wireless Local Area Network (WLAN) undergoes a formal design and configuration analysis, one that ensures the following operational, performance, security, and legal | regulatory compliance requirements are adequately met.

- **Operational:** Properly identifying personnel involved in all aspects of [company name]'s entire WLAN platform, such as the individuals responsible for its initial development and deployment, to a list of authorized end-users of such wireless technologies. Additionally, identifying critical operational procedures relating to change management, configuration management, vulnerability management, continuous monitoring, and other applicable areas. One of the most important measures to identify and determine operationally, is the type of WLAN being configured and deployed- specifically - is it to be used internally by authorized users, or externally, for guests.

- **Performance:** Identifying baseline parameters for signal strength, connection speeds, bandwidth usage, and other critical metrics.

- **Security:** Identifying the safe and secure placement of all physical WLAN devices, such as wireless access points (AP, also referred to as WAP), and all associated wired network devices. Additionally, identifying the following:

  - affect on any other networks currently in place, both wired and wireless.
  - issues with dual connectivity.
  - minimum acceptable encryption protocols for transmission of sensitive and confidential information (i.e., WPA, WPA2).
  - initial installation and deployment hardening procedures.
  - incident response measures for security breaches externally, the use of rogue AP's, and many other considerations.

- **Legal | Regulatory:** Identifying all regulatory compliance laws, legislation, mandated, and industry specific directives that impose various operational and security requirements when implementing WLAN technologies. This is particularly important if [company name] is to send or receive any sensitive and confidential information over wireless platforms.

Provisioning and Hardening

Initially implementing a WLAN requires adherence to the following stated guidelines for ensuring the safety and security of the wireless platform itself, along with ensuring the confidentiality, integrity, and availability (CIA) of [company name]'s overall information systems landscape:

- **Secure Deployment:** All WLAN devices and supporting resources, such as wireless access points, and other network devices, are to be positioned in a manner for ensuring unauthorized physical access and modification. Additionally, they are to be secured with approved fixtures and other necessary apparatuses for mitigating any unnecessary movement. Additionally, the WLAN platform itself is to be logically | physically segregated from the corporate | internal wired network, which can be achieved by utilizing firewalls and other access control methods.

- **Asset Inventory:** Once all WLAN devices are safely secured, a complete asset inventory is to be taken, documenting all necessary information, such as physical location, and corresponding unique identifiers (i.e., hostnames, serial numbers, etc.).

- **Configuration of Wireless Access Points:** The following measures are to be undertaken regarding WLAN platforms:

  - Change default administrator settings, such as username and password, along with implementing strong, unique administrative passwords (i.e., alphanumeric, case sensitive, etc.) for all wireless access points.
  - Change any default IP addresses also.
  - Configure SNMP and NTP accordingly.
  - Configure wireless modes to support only the one (1) primary - and industry approved - wireless networking standard.
  - Change vendor default settings for Service Set Identifier (SSID) to a completely new network name, but also one that does not openly identify or provide any critical [company] name information. Specifically, the SSID character string is not to reflect company name.
  - Use a "closed network" concept, whereby the SSID is actually not broadcasted (if allowable), rather, it must be entered into the client application.
  - If the SSID must be broadcasted, create a healthy balance of allowing all authorized users to receive such signals, but not the point where unauthorized parties can potentially view such information.
  - Remove all unnecessary and insecure services and protocols from all WLAN devices, such as the wireless access points and any all other associated wired network devices.
  - For all remaining services and protocols, implement the concept of "least privileges".
  - Implement MAC Address filtering on wireless access points.
  - Use the strongest encryption algorithm currently available (WPA2), and use other forms of encryption as needed, such as VPN, SSL | TLS, etc.
  - Protect all sensitive wireless access points information, such as administrator passwords, SSID password, keys, etc. with approved security measures, such as encryption itself.
  - Enable logging features and ensure that all logs and audit trails are sent to a remote logging server and retained as necessary (i.e., regulatory compliance laws, etc.). Information captured should include, but not limited to, the following: source\destination IP addresses, MAC addresses, user logon information (i.e., time, username, etc.), user logoff information
  - Enable usage parameters, such as time-out sessions.
  - Disable wireless access points during non-business hours, such as nights, weekends, holidays, etc.

  - Ensure appropriate network security protocols are in place for helping ensure the overall safety and security of all WLAN platforms. Specifically, for internal, corporate WLAN's, use appropriate layered defense mechanisms, such as firewalls, intrusion detection systems, etc.

- **End-User Security:** Access to [company name] WLAN environments requires the use of anti-virus on all laptops, desktops, and other workstations. Additionally, because information often sent via wireless can be deemed sensitive and confidential, all users are to abide by [company name]'s wireless security general guidelines, responsibilities, and acceptable user as defined below.

Rogue AP's
Wireless Access Points installed by users onto the organization's WLAN without the knowledge or consent of authorized personnel are deemed "rogue" and are in violation of information security best practices. Because Rouge wireless access point have not gone through an extensive provisioning and hardening process, they pose an immediate threat to the safety and security of [company name] system resources, and are to be promptly disabled upon being identified. Physically removing the WAP apparatus and/or shutting down connectivity (such as the switch port, blocking an IP address, etc.) are considered acceptable. An approved wireless analyzer - one capable of detecting all wireless access points - is to be used on a regular basis for both confirming all allowed AP's, along with identifying Rogue AP's.

Wireless Handheld Devices
The continued growth and use of wireless handheld devices - small, mobile devices capable of sending, receiving, and storing information (much of it deemed sensitive and confidential) requires implementation of the following security measures:

- **Approved Devices:** Authorized I.T. personnel at [company name] are to exhaustively research all applicable devices for ensuring they meet minimum baseline security standards, while also providing necessary embedded security features, along with vendor support.
- **Authentication:** Such devices must contain features for entering certain credentials (i.e., usernames, passwords, biometrics, etc.) allowing them to be used by authorized personnel. Lost, stolen or misplaced devices can immediately be accessed by unauthorized parties without such security provisions in place.
- **Wipe Programs:** If possible, implement secure remote wipe programs that allow data to be removed in the event such devices are lost, stolen, misplaced.
- **Encryption:** All wireless handheld devices used for sending, receiving, and storing information are to have encryption enabled at all times.
- **Provisioning and Hardening:** Remove all unnecessary services and protocols, along with not allowing third-party applications to function (as applicable). Additionally, utilize anti-virus, personal firewalls, intrusion prevention systems, file integrity monitoring (FIM) as necessary.
- **Bluetooth:** Disable Bluetooth when not in use

Access Rights

Administrative access rights to [company name] WLAN platforms are limited to authorized personnel only, such as systems administrators, network engineers - individuals responsible for the overall design, configuration, implementation, maintenance, and monitoring of wireless access points. End user access rights include all employees and other applicable third-parties as designated by [company name]. Additionally, all access must include the user of a username and password for helping prevent unauthorized access to [company name] wireless local area networks.

Wireless Security Threats
The use of wireless security provides convenience, portability, and flexibility, but also numerous security threats, for which all individuals at [company name] are to be aware of, such as the following:

- **Spoofing:** More specifically - MAC spoofing - can occur whereby MAC addresses are obtained by unauthorized parties and used (in conjunction with other software tools) for gaining access to a network.
- **Denial of Services (DoS):** A concept whereby an attacker deliberately floods a network - in this case, a WLAN platform - with requests and other network related activities, resulting in the loss of use for intended users, and possibly even the platform "crashing".
- **Eavesdropping and Tampering:** Intercepting, capturing and/or modifying data and information being sent or received over the WLAN platform

Continuous Monitoring
Security for all [company name] WLAN platforms is highly dependent on comprehensive continuous monitoring practices, such as the following:

- Changing the SSID every ninety (90) days.
- Changing administrator wireless access points passwords every ninety (90) days.
- Changing end-user wireless access points passwords every ninety (90) days.
- Updating of firmware and related patches and security updates as necessary.
- Reviewing all log files on a regular basis and reporting issues, concerns, constraints immediately.
- Reviewing access rights on a regular basis, both administrator access rights, along with end-user access rights.