

## About this template:

Joel Barrett, a Systems Engineer and member of the Enterprise Wireless LAN Technology Leadership Program (TLP) at Cisco Systems, developed this Wireless LAN Security Policy Template.

The purpose of this template is to provide enterprises with a starting point for developing a security policy to apply to the implementation of a wireless network, whether that implementation is yet to be completed, or has been installed already. The point being that any organization that uses wireless LAN technology needs to have a security policy to address the security issues inherent to any wireless LAN installation.

This template is fully printable, can be used on a PDA, allows extraction of contents, but does not allow for editing of the document.

## Introduction

Use the following template to build a comprehensive corporate wireless LAN security policy. Each section and subsection contains a heading and then brief instructions or suggestions for what that section should contain. The final result should be integrated with the existing corporate security policy. Organizations may not need all of the sections listed in this template, but we have included a comprehensive list to choose from. The policy may need revision when new wireless network vulnerabilities and/or solutions arrive in the market place. An electronic version (Adobe PDF) of this template is available when you subscribe to the CWNP e-mail newsletter.

## General Policy

This first section, General Policy, is used as an introduction to why the organization is adding a wireless section to their corporate security policy (its purpose) and what role this policy will play in keeping the network safe from intrusion. Even if the organization has no wireless capabilities, a wireless security policy should be in place to address a minimum of rogue equipment discovery.

### Introduction

An introductory section on what the General Policy section covers and how it applies to the organization.

### Statement of Authority

Define the authority that put this policy in place.

### Executive Sponsorship

List the executive sponsors who back this policy and their contact information.

### Emergency Response Team

Large organizations usually have an Emergency Response Team to handle corporate security issues for both facility and network emergencies. List ERT network representatives and the team's contact information.

### Applicable audience

Define the audience to whom this policy applies, including employees, visitors, and contractors.

Scaled down versions of the Wireless LAN Security Policy may be needed for IT staff, end users, visitors, and contractors as an easy-to-read type of "To Do" and "Not To Do" list.

## Violation reporting procedures and enforcement

Part of the security policy must address policy enforcement. When policy is violated, there must be a procedure in place to address what actions the organization will take against the individual that violates policy directives. Define and describe what will be done to reinforce policy directives after a violation and what reports will be written by whom and whom they will be given to.

## Risk Assessment

### Asset Protection

#### Sensitive Data

List and discuss the organization's intellectual property, trade secrets, identity information, credit card information, health information, customer databases, and any other information stores that could be jeopardized by wireless network compromise.

#### Network Services

List and describe email, file, database, directory, custom application services, Internet connectivity, web-based applications, and virus and intrusion detection services that could be compromised by network infiltration.

### Threat Prevention

Explain the steps necessary to reduce or prevent wireless network threats, such as:

- Denial of Service (DoS)
- Equipment Damage or Theft
- Unauthorized Network Access
- Credit Card Fraud
- Identity Theft
- Corporate Secret Theft
- Personal Information Exposure
- Malicious Data Insertion

### Legal Liabilities

Document legal liabilities that could be incurred in the event of a wireless network compromise and how to react to each type of situation appropriately. These liabilities should also include third party attacks and illegal data insertion.

Note that if exposure to legal liabilities presents a problem that could cost significant amounts of time and money due to an intrusion, then adequate resources should be proactively applied to the security weaknesses.

## Costs

Management must consider costs involving people, training, and equipment when implementing wireless LAN security solutions. Keeping quality employees who fully understand the network and its vulnerabilities is especially important. Training is continually required for installation and configuration tasks. Training is imperative to maintaining network operations, end-user capabilities, and security solution upgrades.

This section should give way to Finance & Budget documentation for extensive details, but should outline the importance of appropriate spending to assure security levels are appropriate. List the various expenses that are expected in implementing and maintaining proper wireless network security.

## Impact Analysis

An Impact Analysis should be performed so that administrators understand the degree of potential loss involved in a network compromise. The following items, as a minimum, must be considered during the Impact Analysis:

- Financial Loss
- Data Loss
- Loss of Customer Confidence
- Reputation Damage
- Regulatory Effects

Policy should address accessing the network from outside the organization, especially from public access locations (i.e. wireless hot spots).

## Security Auditing

### Independent Testing

This section is about hiring external consultants to perform independent security testing of wireless network systems. This step is often taken after internal resources and knowledge have been exhausted or to get a fresh perspective on security design and solution selection. The tests allowed to be performed by the consultant should be documented and cleared through internal legal channels. Any anticipated vulnerabilities or limitations of the security solutions chosen should be documented before the auditor begins any testing.

### Sources of Information

There are many tools hackers can employ to infiltrate wireless networks. Audits should employ as many of these tools as possible:

- Wireless LAN Discovery
- Password Capture & Decrypt
- Share Enumerators
- Network Management & Control
- Wireless Protocol Analyzers

- Manufacturer Defaults
- Antennas & WLAN Equipment
- OS Fingerprinting & Port Scanning
- Application Layer Analyzers
- Networking Utilities
- Network Discovery Tools
- RF Jamming Tools
- Hijacking Tools
- WEP Decryption Tools
- Operating System Exploit Tools

List and describe the tools that are, have been, or will be used in auditing the wireless segment of the network.

## Functional Policy – Guidelines and Baselines

### Policy Essentials

#### Policy Change Control and Review

##### Contacts and Responsibilities

Include the specific contacts and their responsibilities for policy change control management.

##### Change Management Procedures

List the specific procedures for making changes to organizational policy.

##### Change Control Enforcement

Describe the procedures used when enforcing organizational policy change control.

#### Password Policy

##### Guidelines

Create guidelines that help users implement strong passwords and help administrators enforce password policy.

##### Password Implementation

If passwords are used as a security mechanism, set password policies for the following network devices as a minimum.

- Access points
- Wireless client software
- Other wireless infrastructure devices
- Windows platforms
- Linux/Unix platforms

- VPN solutions
- Applications

## **Networking Staff and End User Employee Training Requirements**

### **Networking Staff**

Explain training requirements for the networking staff.

### **End Users**

Explain training requirements for end users.

## **Non-Employee Wireless Access**

### **Visitors**

Explain access restrictions for visitors.

### **Consultants**

Explain access restrictions for consultants.

## **Acceptable Use Policy**

### **Acceptable Use**

Explain acceptable uses of the wireless network.

### **Unacceptable Use**

Explain unacceptable uses of the wireless network.

### **Violation Enforcement**

Define the methods used to enforce the Acceptable Use Policy.

## **Staging, Implementation, and Management Procedures**

Describe the procedures that will be used to maintain consistency when staging, implementing, and managing wireless network devices. These procedures must be readily available and up-to-date when used by support staff to manage the devices. This section may include checklists, interface types used for management, and how the wireless infrastructure will be installed.

## **Auditing and Compliance**

### **Internal recurring process by support staff**

Support staff must perform penetration testing and reporting, vulnerability scanning, and risk assessments on an ongoing basis. Audits should follow the

policies established in the Risk Assessment section of the Wireless LAN Security Policy. Define established timelines and processes for recurring internal audits.

#### **External periodic process by independent professionals**

Independent professionals should be considered as a valid periodic method of performing penetration testing and reporting, vulnerability scanning, and risk assessments. Define established timelines and processes for recurring external audits.

## **General Guidelines**

### **Security Checklist**

Create a security checklist that addresses the expectations of the security policy. This checklist will be used during product staging, implementation, and management to verify configuration parameters are set correctly. This checklist should comply with the Baseline Practices section below.

### **Available Network Resources**

Define the restrictions that wireless users have compared to wired network users regarding use of existing network resources. It is not always necessary to give wireless users the same level of access to network resources as wired users.

### **Asset Management**

Describe the asset management practices in place and how they affect the wireless network. This may include an intrusion detection and management software package or similar asset management tool.

#### **Periodic Inventory**

Show the organization's inventory schedule and the team responsible for the schedule.

### **Change Management**

Make appropriate annotations about how existing change management procedures should include wireless LAN infrastructure devices. This should list the steps to be followed in order to properly implement a change on the wireless network so as to assure adherence with all sections of this policy.

### **Spot-checks & Accountability**

Perform regular spot checks to prevent rogue access points and similar devices and to verify policy compliance. End users and network staff should be held accountable to the corporate policy. Establish timelines and processes for conducting spot checks.

## Baseline Practices

Establish baseline practices to help create operating procedures and implementation checklists for wireless LAN equipment and security. These areas need to be considered:

- Access point default SSID modification
- MAC filtering
- Use of static WEP
- Default access point configuration modification
- Firmware upgrades for wireless network equipment
- Rogue equipment
- Outdoor bridge security
- RF cell sizing and AP placement
- SNMP configuration
- Discovery protocol configuration
- Remote access configuration
- Client configuration
- IP services configuration
- AP network connectivity
- Pre-deployment staging and testing
- Equipment installation

## Functional Policy – Design and Implementation

### Interoperability

Consider solutions that interoperate and document how interoperability affects purchasing decisions. For example, if 128-bit WEP is chosen as a security solution and multiple wireless LAN infrastructure equipment providers are used, then interoperability testing should be performed before an enterprise rollout is attempted and before a large amount of equipment is purchased.

### Layering

If solutions that use different layers of the OSI model are used, it is important to document which solution types will be used and to assure that they have been tested together. An example of this is using 802.1x/EAP (layer 2) solutions with IPSec (layer 3). Define policy for implementing layered security solutions.

### Segmentation & VLANs

Wireless LANs should be segmented from the wired network backbone by an appropriate security solution. Wired and wireless VLANs offer a method of segmenting users and networks. The importance of segmentation should be explained here, and the type(s) of segmentation solution required to properly secure the network should be listed. Any necessary security and mobility features should be documented here.

## Authentication & Encryption

Choose and document authentication and encryption types based on existing implementations, data sensitivity, scalability, availability, and access control.

### Existing Implementations

Authentication system integration with existing user databases and authentication systems and support for the latest standards, security features, and protocols is paramount. Existing equipment may not be able to support the latest available encryption, so an evaluation of the level of security provided by these more legacy devices is warranted. Describe and document the current level of encryption on existing systems and devices.

### Data Sensitivity

Define and document authentication and encryption solutions that support the required level of security. Keep in mind that authentication systems do not typically provide data payload encryption. In most cases, authentication and data encryption must be handled by separate mechanisms.

### Scalability & Availability

Security solutions should be scalable and provide a high degree of availability for users. Wireless networks allow employees to be mobile which means that new ways of using the network will be found. This will translate into increased network usage and dependency on the network. The network's design should lend itself to ease of growth at a reasonable cost. Define and describe the levels of scalability and availability that are required for the wireless network to grow with the organization.

### Access Control

Having a wide range of device types may dictate a degree of flexibility in choosing security solutions. Create corporate security solutions that can handle access control for a variety of wireless network device types, manufacturers, and operating systems. Solutions may include client and server software applications that run on various operating systems, authentication and encryption appliances, and a plethora of infrastructure devices such as access points, workgroup bridges, and wireless bridges. Access may be controlled based on roles, groups, device types, etc. Define and document the different levels of access control to be implemented on the wireless network segment.

# Functional Policy – Monitoring and Response

## Physical Security

Address unauthorized visitors in the facility's physical security policy. Physical access and security of wireless infrastructure devices is extremely important in preventing hackers from entering the facility to place their own wireless devices onto the network and to keep thieves from stealing equipment or accessing console ports of infrastructure devices. Define and describe the facility's physical security required as a result of implementing the wireless network.

## Rogue Access Points & Ad Hoc Networks

Prevent rogue access points and Ad Hoc networks inside the corporate work area. A well-defined wireless security policy can help prevent most rogue access points – whether placed by employees or intruders. Make periodic manual scans or have a wireless IDS in place to detect unauthorized equipment. Define and describe the regularity and processes for preventing and detecting rogue wireless devices.

## RF Jamming

RF jamming should be addressed so that network administrators understand how to recognize and appropriately react to unintentional and intentional jamming of any kind – to include spread spectrum and narrowband. Explain how RF jamming is accomplished and explain appropriate preventative or responsive steps.

## Data Flooding

Give end users a clear definition of what it means to be a good wireless network user. End users may inadvertently flood the wireless network when downloading large files. Help end users understand what should and should not occur over the wireless LAN. Explain baselining as a task to be performed by the network administrator, and reinforce the importance of maintaining baselines over time and changes to the network. Explain how baselines are to be used as a comparative tool to help identify network attacks. Explain how data flooding is accomplished, and list any preventative steps.

## Social Engineering

Ensure employees are aware of the data they are making available to others and what hackers might do with the knowledge they gain from that data. Train end users in the proper handling of social engineering tactics, such as:

- Dumpster diving
- Phone calls
- Email
- Instant messaging

- Onsite Visits

## Prevention

Teach employees how to prevent intrusion attempts by verifying identification, using secure communication methods, reporting suspicious activity, establishing procedures, and shredding corporate documents. Define established procedures for employees to report or respond to various types of attacks.

## Audits

Employ external consultants to perform periodic audits and social engineering attempts to test employees and the network security. Define regularity of audits by external consultants.

## Reporting

Develop clear procedures for who is responsible for generating reports and who reviews the reports. Timely, accurate, and comprehensible reports are essential in future attack prevention and pinpointing hacker activity. Define and describe the types of reports, details within the reports, and proper archival of all reports for historical reference.

## Response Procedures

Define the steps to take after an intrusion has been recognized. Recommended steps should include a minimum of the following:

- Positive identification
- Confirmed attack
- Immediate action
- Documentation
- Reporting



## Appendices

### Glossary

Include a glossary to define words readers may not understand or those that require further clarification.

### Whitepapers

Include any applicable industry whitepapers that may help during implementation, analysis, prevention, or recovery.

### Education / Certification

List any classes, self-study materials, and certifications that would be beneficial to employees (end users and IT staff) toward the goal of securing the wireless network.