

Wireless Communication Policy

1.0 Purpose

This policy prohibits access to <Company Name> networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by InfoSec are approved for connectivity to <Company Name>'s networks.

2.0 Scope

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

3.0 Policy

3.1 Register Access Points and Cards

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by InfoSec. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with InfoSec

3.2 Approved Technology

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

3.3 VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

3.4 Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms

User Authentication

Definitions

A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History

July 10, 2003, Section 3.4 Added

July 6, 2003, expanded to support CDI Initiative, Stephen Northcutt