

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

To comply with this policy, wireless implementations must: Maintain point to point hardware encryption of at least 56 bits. Maintain a hardware address that can be registered and tracked, i.e., a MAC address. Support strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

EXCEPTION: A limited-duration waiver to this policy for Aironet products has been approved, if specific implementation instructions are followed for corporate and home installations.

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