Wireless Security Checklist

Wireless Security Provisioning and Hardening Steps				
	Task	**Completed?**	**Date Completed**	**Signature**
Description of Wireless Platform:				
(1).	**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.**			
(2).	**Change any default IP addresses also.**			
(3).	**Configure SNMP and NTP accordingly.**			
(4).	**Configure wireless modes to support only the one (1) primary - and industry approved - wireless networking standard.**			
(5).	**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.**			
(6).	**Use a "closed network" concept, whereby the SSID is actually not broadcasted (if allowable), rather, it must be entered into the client application.**			
(7).	**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.**			
(8).	**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.**			
(9).	**For all remaining services and protocols, implement the concept of "least privileges".**			
(10).	**Implement MAC Address filtering an wireless access points.**			
(11).	**Use the strongest encryption algorithm currently available (WPA2), and use other forms of encryption as needed, such as VPN, SSL | TLS, etc.**			

(12).	**Protect all sensitive wireless access points information, such as administrator passwords, SSID password, keys, etc. with approved security measures, such as encryption itself.**			
(13).	**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**			
(14).	**Enable usage parameters, such as time-out sessions.**			
(15).	**Disable wireless access points during non-business hours, such as nights, weekends, holidays, etc.**			
(16).	**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.**			