Wireless Security Policy

Policy #:

Version #: 1.0

Approved By:

Effective Date:

Purpose:

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of <<Organization Name>>’s wireless infrastructure to a ***reasonable and appropriate level***.

Scope:

This policy applies to <<Organization Name>> in its entirety, including all facilities and systems that process sensitive information.

Policy:

<<Organization Name>> wireless infrastructure must follow these guidelines:

***Design***

* Configure a firewall between the wireless network and the wired infrastructure.
* Ensure that 128-bit or higher encryption is used for all wireless communication.
* Fully test and deploy software patches and updates on a regular basis.
* Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.

***Access Points (AP)***

* Maintain and update an inventory of all Access Points (AP) and wireless devices.
* Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
* Place APs in secured areas to prevent unauthorized physical access and user manipulation.
* The default settings on APs, such as those for SSIDs, must be changed.
* APs must be restored to the latest security settings when the reset functions are used.
* Ensure that all APs have strong administrative passwords.
* Enable user authentication mechanisms for the management interfaces of the AP.
* Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
* Turn on audit capabilities on AP; review log files on a regular basis.

***Mobile Systems***

* Install anti-virus software on all wireless clients.
* Install personal firewall software on all wireless clients.
* Disable file sharing between wireless clients.

Responsibilities:

The Security Officer has the responsibility to ensure that all wireless end systems such as laptops and PDAs, as well as all APs are deployed based on policy requirements. The Security Officer must review log files from APs and other systems on a regular basis. The Security Officer must send reminders to all employees about wireless network security.

Compliance:

Failure to comply with this or any other security policy will result in disciplinary actions as per the HR XXXXX Policy. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

Procedure(s): None

Form(s): None

References:

* The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
* International Standards Organization (ISO 27002).

Contact:

John Doe, Security Officer

1234 Anystreet

Anywhere, WY XXXXX

E: John.doe@anywhere.com

P: 307.XXX.XXXX

F: 307.XXX.XXXX

Policy History: Initial effective date: July 1, 2015