Stark County Board of Developmental Disabilities

Policy 6.19 Wireless Access	Effective: 4/28/15
Chapter 6: Information Technology	Page 1 of 4

WIRELESS ACCESS

POLICY

Wireless communication is quickly becoming the standard of connecting devices at the Board.
In the past, wireless access was the exception; it has now become the norm. However, while wireless access can increase mobility and productivity of users, it can also introduce security risks to the network. These risks can be mitigated with a sound Wireless Access Policy.

The purpose of this policy is to state the standards for wireless access to the Board's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the Board wishes to take to secure its wireless infrastructure.

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, switches, and anything else capable of transmitting or receiving a wireless signal.

Historical Resolution Information		**Reviewer(s):**
Date	**Resolution Number**	Director of IT
10/26/10		
3/28/15	03-19-15	

WIRELESS ACCESS

PROCEDURE

I. **Physical Guidelines**

Access points should be located in ceilings and hidden by ceiling tiles if at all possible. They should be securely bolted to the ceiling trusses as to make them difficult to remove. External access points should be mounted inside the building with a remote external antenna ran to the outside for coverage. Note that this practice will not always be able to be used in the case of warehouse and shop floor environments with open ceilings. The access points should be mounted high enough in these areas as to not allow access to the device without a ladder or some type of lift.

II. **Configuration and Installation**

The following guidelines apply to the configuration and installation of wireless networks:

A. **Security Configuration**

• The Service Set Identifier (SSID) of the access point must be changed from the factory default.

• The SSID should not be broadcast as a best practice. This adds a layer of security by requiring wireless users to know the SSID in order to connect to the network.

• The wireless access point should utilize 802.1x authentication with radius for production network,

• Encryption must be used to secure wireless communications. The strongest available algorithm must be used (e.g., WPA rather than WEP).

• Administrative access to wireless access points must utilize strong passwords.

• All logging features must be enabled on the Board's access points.

• Wireless networking should require users to authenticate against a centralized server. These connections should be logged, with IT staff reviewing the log regularly for unusual or unauthorized connections.

• Wireless LAN management software should be used to enforce wireless security policies. The software must have the capability to detect rogue access

points.

• Guest access should require the user to provide at a minimum their name and email address to access the guest network. This provides IT with a log of who is using the guest access.

• Guest access networks should be segmented and isolated from production networks. Guest networks should only provide internet access and its bandwidth should be throttled as to not interfere with day to day business operations of staff.

• Contractor access networks should be setup to allow for contractors and vendors that need access to production systems for projects. These networks will require special configuration from IT to get users connected. Strict control of these networks should be enforced.

B. **Installation**

• Software and/or firmware on the wireless access points and wireless network interface cards (NICs) should be updated prior to deployment.

• Wireless networking must not be deployed in a manner that will circumvent the Board's security controls.

• Wireless devices must be installed only by the Board's IT department or an IT contractor, vendor, or partner.

• Channels used by wireless devices must be evaluated to ensure that they do not interfere with Board equipment.

III. **Accessing Confidential Data**

Wireless access to confidential data is permitted as long as the access is consistent with this and other policies that apply to confidential data.

IV. **Audits**

The wireless network must be audited quarterly to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, SSID broadcast, and use of strong encryption.

V. **Applicability of Other Policies**

This document is part of the Board's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

VI. **Enforcement**

This policy will be enforced by the IT Director and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of Board property (physical or intellectual) are suspected, the Board may report such activities to the applicable authorities.

Definitions

Mac Address Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

SSID Stands for Service Set Identifier. The name that uniquely identifies a wireless network.

WEP Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.

WiFi Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.

Wireless Access Point A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

Wireless NIC A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

WPA Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.