Wireless Access

Purpose

The purpose of this procedure is to limit and restrict the number of wireless access points, within the organization's premises, connecting to Bellevue School District (BSD) internal network or related technology resources via any means involving wireless technology.

The overriding goal of this procedure is to protect BSD's technology-based resources (such as district data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing district technology resources must adhere to district-defined processes for doing so, using district-approved access points.

Scope

This procedure applies to all BSD employees, including full-time staff, part-time staff, students, contractors, freelancers, and other authorized agents who utilize mobile computers to access the organization's data and networks via wireless means. Wireless access to enterprise network resources is a privilege, not a right. Consequently, enrollment/employment at BSD does not automatically guarantee the granting of wireless access privileges.

Access Points

A. BSD is committed to providing authorized users with wireless access to the Internet, BSD networks and systems, as well as other district resources. In order to make this convenient service available to end users, the Technology (Tech) Department must install "access points" in and around the premises wherever wireless access to district resources is designated. These access points are generally small, antenna-equipped boxes that connect directly to the local area network (LAN), converting the LAN's digital signals into radio signals. The radio signals are sent to the network interface card (NIC) of the mobile device (e.g. PDA, laptop, etc.), which then converts the radio signal back to a digital format the mobile device can use.
    1. As the number of wireless connections increases, so too does the danger of "rogue" access points being surreptitiously installed. Rogue access points are antennas that are installed without the knowledge or permission of BSD, used by hackers, internal employees, or trespassers to gain illegal access to the district network and Internet connection for the purposes of sabotage, spamming, district espionage, personal gain, and so on.
    2. All wireless access points within the district firewall will be centrally managed by BSD's Tech Department and will utilize encryption, strong authentication, and other security methods at the Tech Department's discretion. Addition of new

wireless access points within district facilities will be managed at the sole discretion of the Tech Department. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organizational premises, is strictly forbidden.

B. BSD Service Set Identifier (SSID) List
    1. **BSDSecure** – Is for BSD owned devices. It uses WPA2 and 802.1X for Auth. This SSID will have access to all District internal Networks.
    2. **BSDPersonal** – Is for Non-BSD owned devices and users that have a valid BSD Active Directory account. It uses WPA2 and 802.1X for Auth. Staff and Students can access BSDPersonal, they will have controlled access to District Networks: district web based applications and the Internet. Both groups will be filtered at the appropriate level when accessing sites on the internet, this is handled by the firewall and no additional configuration is required on the personal device.
    3. **BSD Guest Access** – Is for users that have non-BSD owned devices and no Active Directory account (General Public). It is offered with no guarantees of reliability, security or privacy. During school hours it is filtered at a student level, after hours staff filters are used. This is an open network.
    4. **BSD405** – Is for District Machines that use a local logon. It uses WPA2 and a Pre-Share Key for authorization This SSID should be used in rare cases.

Procedure Restrictions

1. All wireless clients and devices shall be equipped with a host-based personal firewall and anti-virus software. The user shall update these applications as required, and will not reconfigure them in any way.
2. Whenever necessary, the Tech Department will conduct a site survey to determine the appropriate placement of new or additional access points. All installations will be in compliance with all local safety, building, and fire codes.
3. All access point broadcast frequencies and channels shall be set and maintained by the Tech Department. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.
4. Use of the wireless network is subject to the same guidelines as BSD's Acceptable Use Procedure (AUP).
5. BSD's Tech Department cannot guarantee 99.999 percent availability of the wireless network, especially during inclement weather. Nevertheless, the Tech Department will make all possible network adjustments within the supported radio frequency spectrum.
6. The Tech Department reserves the right to turn off without notice any access point connected to the network that it feels puts the district's systems, data, users, and equipment at risk.

7. The wireless access user agrees to immediately report to his/her manager/principal and BSD's Tech Department any incident or suspected incidents of unauthorized access point installation and/or disclosure of district resources, databases, networks, and any other related components of the organization's technology infrastructure.

Date: 09.14