DRAFT

Wireless Security Policy

Southwest Area Technology Team Collaborative Draft Policy
Draft 1: 10/27/08

1. Purpose

This policy establishes standards that must be met when wireless communications equipment is connected to <District Name> networks. The policy prohibits access to <District 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 Information Security are approved for connectivity to <District Name>'s networks.

2. Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, Bluetooth equipped devices, and 802.15 devices etc.) connected to any of <District 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 <District Name>'s networks do not fall under the purview of this policy.

3. Policy

3.1 Approved equipment

All wireless LAN access must use district-approved products and security configurations. All network equipment, both wired and wireless, must be purchased & installed by District technology personnel.

3.2 Monitoring of uncontrolled wireless devices

All District locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect, classify, and disrupt communication with unapproved (rogue) wireless access points. All District locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect the presence of wireless devices forming a

connection between the network and any wireless network. This would include laptops that are serving as a bridge between wired and wireless networks or computers participating in ad-hoc or peer-to-peer wireless networking. In District locations where wireless LAN access has been deployed, whenever possible, wireless intrusion detection systems will be deployed to monitor for attacks against the wireless network.

3.3 Authentication of wireless clients

All access to wireless networks must be authenticated. The District's existing strong password policy must be followed for access to wireless networks. The strongest form of wireless authentication permitted by the client device must be used. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network. Any District user with an account in a District user database shall be able to authenticate at any District location where wireless access is present.

3.4 Encryption

All wireless communication between District devices and District networks must be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement. The strongest form of wireless encryption permitted by the client device must be used. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.

3.5 Access control policies

- Access to District network resources through wireless networks should be restricted based on the role of the user.
- Unnecessary protocols should be blocked, as should access to portions of the network with which the user has no need to communicate.
- Access control enforcement shall be based on the user's authenticated identity, rather than a generic IP address block. This is also known as "identity-based security." The access control system

must be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.
- Access control rules must use stateful packet inspection as the underlying technology.

3.6 Remote wireless access

Telecommuting employees working from remote locations must be provided with the same wireless standards supported in District offices. Employees should be discouraged from connecting District computers though consumer type wireless equipment while at home in lieu of District-provided equipment. Remote users outside of the district network must connect to district resources using a secure connection such as a VPN.

3.7 Client security standards

- All wireless clients must run District approved anti-virus software that has been updated and maintained in accordance with the District's anti-virus software policy.
- All wireless clients must run host-based firewall software in accordance with the District's host security policy.
- All wireless clients must have security-related operating system patches applied that have been deemed "critical" in accordance with the District's host security policy.
- All wireless clients must be installed with District-standard wireless driver software. Clients not conforming with minimum security standards will be placed into a quarantine condition and automatically remediated. Client operating systems that do not support client integrity checking will be given restricted access to the network according to district requirements.

3.8 Wireless guest access

- Wireless guest access will be available at all facilities where wireless access has been deployed.
- All wireless guest access will be authenticated through a web-based authentication system (captured portal).
- A single username/password combination will be assigned for all guest access. The password for guest access will be changed monthly and distributed to local facility managers. Special accounts may be

created for guests on a request basis. Access must be arranged at least 24 hours before planned access.

- Wireless guest access is available from the hours of ____ until ____ .
- Wireless guest access is bandwidth limited to __Mb/s per user.
- Guest access will be restricted to the following network protocols:
    - HTTP (TCP port 80)
    - HTTPS (TCP port 443)
    - IMAP (TCP 143)
    - POP (TCP port 110)
    - IKE (UDP port 500)
    - IPSEC ESP (IP protocol UDP 50)
    - PPTP (TCP port 1723)
    - GRE (IP protocol 47)
    - DHCP (UDP ports 67-68)
    - DNS (UDP port 53)
    - ICMP (IP protocol 1)