Spring Hill School District Wireless Security Policy

Spring Hill School District uses an enterprise wireless solution to provide management and an additional level of security to the wireless network. Access to wireless management is limited and requires strong authentication. To minimize potential exposure and risk of district data, including but not limited to loss or corruption of sensitive, confidential or financial data, Spring Hill School District has the following security measures in place for Wireless Security:

- To prevent unauthorized access, the district requires faculty, staff and students to use strong passwords to connect to SSIDs. Certain SSIDs are not broadcast, and MAC address filtering is used. All default passwords have been changed. On occasion, when guest access is required, the guest network is activated and the password is given out. The guest network is deactivated when not in use and the password is changed before reactivation.
- Mobile devices are managed through the Meraki Mobile Device Management System. Chromebooks are also managed through the Google Admin Console. Through the use of these management systems, devices can be associated with specific SSIDs, apps pushed out, and devices locked or wiped.
- Access to wireless management is limited to the technology department personnel using specified accounts with strong passwords.
- Automatic updates are configured to keep access point software patched. The network administrator checks the management dashboard for updates monthly to ensure that updates are installing correctly.
- Faculty and staff are reminded yearly that all devices should be approved by the technology department and/or administration prior to connection to the Spring Hill School District Computer Network.
- All personal devices should be checked by technology personnel. Unknown devices can be blocked at the wireless management console or assigned a custom profile.
- This policy is included in the Acceptable Use Policy that all employees sign at the beginning of each school year.
- The Spring Hill School District wireless network scans for rogue devices in real time, contains the device, and reports any rogue access points to the technology staff.
- At the end user level, all district owned machines have anti-virus and anti-malware utilities installed where applicable to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.
- A warning banner is displayed on each district owned machine informing users of the acceptable use of the network and possibility of monitoring. Wireless access users are informed via a splash page login.
- At the wireless access point, firewall rules, filtering rules, and application rules, as well as an encrypted password for the SSID are configured to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.
- At the district level, all devices are behind a firewall and a content filter that applies real-time monitoring which is used to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.
- As an ongoing effort, the district will continue to follow the Best Practices Statement from DIS (http://www.dis.arkansas.gov/policiesStandards/Documents/BP-70-010_wireless_best_practices.pdf).