East End School District
Wireless Security Policy

East End School District Technology Department conducted a risk assessment to identify possible risks of the wireless network in its current state. The district uses an enterprise wireless solution to provide management and an additional level of security to the wireless network. All access points are located in physically secure locations, and 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, East End 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. SSID is not broadcast, and MAC address filtering is in effect. All default passwords have been changed. On occasion, when guest access is required, the guest network is enabled and the password is given out. The guest password is changed regularly. Passwords are regularly changed to ensure access is gained only by authorized users.
- Access to wireless management is limited to the technology director using an account with a strong password.
- Automatic updates are configured to keep access point software patched. The network administrator manually checks for updates monthly to ensure that updates are installing correctly.
- This policy is included in the Acceptable Use Policy that all employees sign at the beginning of each school year.
- The network administrator checks for rogue devices monthly, and unidentified devices are denied access.
- All district buildings have secure access requiring a physical key to gain entrance. Access control is limited based on employee position.
- Wireless access points are located in physically secure locations.
- At the end user level, all district owned machines have anti-virus and anti-malware utilities installed 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.
- A captive portal is in place showing the district's acceptable use policy for users to authenticate to gain access to the wireless network. Each user must log in through the captive portal to have any network resources.
- At the wireless access point, firewall 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).