7200-R Section 1, Network Security

Campbell County School District will:

- Use encryption as much as possible to protect data;
- Use firewall(s) to secure critical segments;
- Use firewall(s) to detect and stop unauthorized intrusion and detection of network level threats;
- Secure Domain Name System (DNS) services to prevent unauthorized use;
- Disable all services not in use or services having a use of which you are not sure;
- Use encrypted protocols when connecting to network equipment wherever possible.
- Avoid using plain text protocols as much as possible; and
- Secure Routing protocols wherever possible (i.e. enable password authentication on protocols).

Campbell County School District wireless infrastructure must adhere to the following guidelines:

- Design
    - Configure a firewall between the wireless network and wired infrastructure.
    - Ensure a Wi-Fi Protected Access 2 (WPA2) with Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) or higher encryption is used for all wireless communication.
    - Test fully and deploy software patches and updates on a regular basis.
    - Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.
- Access Points (AP)
    - Maintain and update an inventory of all Access Points (AP) and wireless devices.
    - Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
    - Place APs in secure areas to prevent unauthorized physical access and user manipulation.
    - Change default settings on APs, such as those for Service Set Identifiers (SSIDs).
    - Restore APs to the latest security settings when the reset functions are used.
    - Ensure all APs have strong administrative passwords.
    - Enable user authentication mechanisms for the management interfaces of the AP.
    - Use SNMPv3 and/or SSL/TLS for web-based management of APs.
    - Turn on audit capabilities on AP, and review log files on a regular basis.
- Mobile Systems
    - Install anti-virus software on all wireless clients.
    - Install personal firewall software on all wireless clients.
    - Disable file sharing between wireless clients.

RESPONSIBILITIES:
The network administrator will be responsible for ensuring network protocols are configured securely and will work with building administrators and technology personnel in developing and securing wiring closets.

ADOPTION DATE: May 11, 2021
LEGAL REFERENCE(S): Children's Online Privacy Protection Act (COPPA), Children's Internet Protection Act, 47 U.S.C. §254 (CIPA); The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) and International Standards Organization (ISO 27002).
CROSS REFERENCE(S): 4374, 4675, 5147, 5276, 5330, 7100, and all sections under 7100-R.
ADMINISTATIVE REGULATION: 7200-R, Sections 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, and 13