SET SEG REMOTE WORK BEST PRACTICES

With remote work, there is an increased risk of employees accessing data through unsecured and unsafe Wi-Fi networks, using personal devices to perform work, and not following general security protocols. Additionally, when employees are working from home, there are often added distractions that could result in inadvertent security incidents. We advise that your district focus on these three areas to help minimize vulnerabilities within your cyber networks and systems.

1 Implement thorough technical controls

Your school should have a protocol in place for secured remote access to district networks. To ensure proper security and access, verify your district's have the following minimum structures in place:

- Remote access to district networks should be through a virtual private network (VPN), which routes the connections through the district's private network, or another encrypted connection mechanism.
- VPNs should be configured with multi-factor authentication (MFA) as an added security layer for private information.
- Your IT Department should ensure firewalls are properly configured and monitor firewall logging to identify attempted or successful connections from unauthorized or suspicious Internet Protocol (IP) addresses.

2 Conduct staff trainings focused on teaching best practices and building awareness

There has been an increased risk of phishing attacks and other social engineering schemes during the COVID-19 outbreak. Attackers are exploiting the COVID-19 outbreak by sending malicious emails to those in geographic areas heavily impacted by the virus. Without adequately training your staff, you're nearly defenseless as human error is the biggest perpetrator in these instances.

Make sure your technology security trainings cover at least these topics:

1. Acceptable use policies
2. The logistics of connecting to the network and appropriate use of Wi-Fi
3. Steps to take if a security incident or other compromise is suspected or identified
4. Cautionary reminders to be careful when opening emails, particularly those that include links or attachments, and to report suspicious emails to the IT department
5. Instruction to avoid using personal devices for work purposes as they present additional cybersecurity risks given the lack of control

3 Organize equipment and device management processes

If your district is leasing out technical devices and equipment to students, make sure you're following best practices to sanitize and prepare devices, download protective software, provide appropriate use instructions, collect release forms, and outline return expectations. To access additional information, resources and templates to properly manage equipment, visit our website.