Working Virtually Field Guide   
Corporate data and information are constantly at risk, we all must be even more vigilant about safely conducting business outside the normal business office.  

|  |
| --- |
| **Keep it to yourself** - Don't share your work computer. Never let anyone, not even your kids use your laptop, and remember your surroundings.  Keep your screen from view by those not permitted to share information with. |
| **Verify it**, even calls from the Help Desk.  Cyber criminals often call employees pretending to be from the IT department.  If you receive an unsolicited call, never give out your password or email information to an unknown contact. |
| **Don’t disable security** - Working virtually brings additional concern for security controls.  Never attempt to disable the virus protection or circumvent our security protections. They are designed to provide you with a secure compute space.  The web browser filtering service is enabled while working virtually which is designed to block malicious websites. |
| **WiFi confidence** - Only use WiFi networks that are secure and require a password.  Use your own internet provider service when connecting to our work network. The company VPN program will protect all communications back to our corporate network.  Always confirm the VPN is logged on. |
| **Lock it up**- Our 15-minute idle timeout policy for screensavers will still apply even when outside the office.  Remember to screen lock your laptop when walking away from your desk and store your computer ou​​t of site at the end of the workday. |
| **Keep it clean –**Abide with our Clear Desk policy,don't leave paper document laying around your virtual workspace for others to see.  And, make sure any work paper documents are shredded before placing in trash bins. |
| **Beware of phishing and text scams** - Even working virtually, phishing efforts will still attempt to bypass our spam filters and find their way to your inbox.  Don't click on links or open unknown attachments from suspicious senders. Your mobile device can be just as vulnerable as a laptop computer.  Never try to open an attachment from an unknown text message.​ |