[Securely] Working From Home

Secure Your Home Network

Most home networks are wireless (Wi-Fi) usually controlled either by an all-in-one device that includes the router and modem or a combination of the two. To secure your network you should do the following:

- **Change the default administrator password.** This is used to configure your network. Default passwords can be easily found on the internet and used by attackers to access your network and devices.
- **Only let people you trust connect to your network.** You can do this by requiring a password to connect to the network. This will also cause traffic between the computer and network to be encrypted.
- **Use strong passwords to protect the network.** You should use strong passwords to access your wireless network and they should be different than your administrator password.

Secure Your Devices & Area

Make sure family and friends understand they cannot use your work devices as they can accidentally erase or modify information, or worse, accidentally infect the device.

- **Always connect to the VPN.** If you are connected to an unofficial network, whether home or public, you should connect to the work VPN.
- **Lock your devices.** If you leave your work device (computer or phone) unattended, it should always be locked.
- **Keep your workspace clean.** If you have been given a work printer in order to print documents at home, you should not leave documents unattended or in view of unauthorized people. This includes family. You should never print work-related documents to a personal printer.
- **Monitor your conversations.** Be conscientious of what may be overheard during calls or meetings. Sharing confidential or otherwise protected information with family, even if by accident, may be considered a breach and be reportable.

Practice Good Hygiene

Even when at home and using your personal network, you should follow good cyber hygiene. This is always true, but especially so when working at home.

- **Only go to websites you trust.**
- **Try to limit high bandwidth activities.** If possible, avoid streaming non work-related videos and music on your work device.
- **Don’t click on suspicious emails, links, or attachments.** Anything like this of a questionable nature should be reported to your security team or service desk.
- **Try to only use work devices for work-related tasks.** Personal use of a reasonable nature may be permitted, but keep in mind that work-issued devices belong to the employer.
- **Do not share your work device or password with anyone.** This includes friends and family.
- **Be cautious about what you share on social media.** Posting a photo on Facebook with confidential info shown in the background is a breach.

BUNCOMBE COUNTY
PEOPLE TO MATCH OUR MOUNTAINS
NORTH CAROLINA

TLP:WHITE information may be shared freely subject to standard copyright rules.