Working From Home Checklist

Keeping Your Business Running

CommWest
Your Communications • Our Business

Business continuity is critical. Businesses, small and large, need to adapt when employees need to work from home (WFH) because of business disruptions, such as a contagion, water break, or building remodel. It is important to remember that you cannot forsake security when adding the remote capability for your employees. If you are considering adding remote capability, we strongly recommend working with a Managed Service Provider (MSP).

Before Sending Employee Home

Do you have the hardware needed to work remotely? Computer, phone, router, and other technology.	
Do employees have access to critical programs, software, tools? How will they be accessing the necessary tools?	
Do employees have the needed remote capability with the business phone system?	
Does the home internet connection have the capacity to handle the increased computer and business phone usage?	
Have you established a remote work policy?	
How will you confirm confidentiality best practices and provide necessary training?	

Securing WFH Connection

Confirm that the VPN configuration and software are updated.	
Restrict access to only necessary networks, data, programs, and software.	
Confirm that all operating systems, browsers, and applications are up-to-date.	
Ensure strong passwords are set and used.	
Remove add-ons for browsers.	
Confirm home Wi-Fi is secure – optimizing “Guest” Wi-Fi when possible.	
Ensure all devices have anti-virus enabled and up-to-date.	

Best Practices

Avoid mixing work and personal activities on the same device.
Use multi-layer security solutions.
Have a backup strategy and follow it.
Be especially aware of potential phishing attacks.
Have a list of IT contacts and their work hours to call in an IT emergency.

Securing WFH Connection

Engage your Managed Service Provider or IT services manager to conduct regular employee training on their responsibility to keep your business technology secure.
Establish email etiquette policies and procedures for all employees.
Keep your team updated and informed on new cybersecurity scams and attacks.

Phones/VoIP • Networks • PC Support • Secure Backup

970.242.8142 • info@commwestcorp.com

www.commwestcorp.com