

**Remote Work Individual Checklist** – Each individual role in an organization has unique variables that need to be factored to help identify whether remote work is feasible and if so, how to enable any remote work solution(s) that will fit respective role remote access needs. This checklist is intended to help guide an organization and individual roles to think through the variables associated with remote access. Thinking through these details can help provide a better experience, help maintain productivity, and operate securely while working from home. Here are recommendations for individuals to Work From Home (WFM).

**Use a Corporate owned and managed device** – The preference for remote work is to use a corporate owned and managed device – desktop or laptop - that has security, backup, management and remote support tools installed to keep you safe and productive.

- Not all applications will work remotely via a web browser or over a VPN. If your role requires the use of an application that falls into this category, an alternate form of remote access will be needed. A Remote Access/Terminal Server or connecting to a corporate device that remains at the office may be required to facilitate effective remote access for these roles.
- Additionally, if taking a corporate desktop to WFH, you may need a wireless adaptor or long Ethernet Cable for connecting to the home network.

**Identify an Effective Workspace to WFH** – working from home can also introduce distractions and can contribute to feeling isolated and/or disconnected from your team. With these tips you can make the WFH experience close to that of working from the office.

- Find or create a space where distractions can be minimized.
- Reliable Internet connection at home or utilize cell phone for Internet connection.
- At least one monitor, two would help with productivity

**Proactively think through Internal & External Communication methods** – Most digital communication – like email, Teams/Skype and Video – will easily work at home, however reviewing how your main phone communication will transfer to your team working from home may need some additional consideration.

- Identify roles that may need a physical or soft phone at home to connect to the office phone system for receiving and making calls. This capability depends on your phone system/hosted system and may require additional configuration and/or licensing.
- Webcam for video calls when necessary – internally and externally
  - Be aware of the background that will display on a webcam
- Personal headset/earbuds (with microphone) for audio/video calls
- Personal cell phone or landline with personal headset/earbuds

**Be Aware of Increased Risks While Working From Home/Remote** - When working from home there are different security layers that are often not present which require additional awareness and diligence – especially for those individuals who are not used to working remotely.

- Corporate Firewalls only protect devices when they are using the Internet from the office – not at home.
- Personal machines present an even greater risk as they do not have the same protections as corporate owned and managed devices have in place.
- Bad Actors KNOW more people are working from home and will try to exploit the known security gaps that exist.
- Educate the individual roles on your team of these risks and encourage additional vigilance and to be extra suspicious of emails with links to keep safe while WFH.