Guidelines & Tips for Employees Working Remotely

Working remotely, whether short-term or permanent comes with many perks, but it also poses many new risks for the security of your organization's data. For example, if an employee-owned device (laptop, PC, etc.) is connected to the company's network and contains a virus or malware, they could be spread to your company's network. Additionally, it becomes more of a challenge to verify the legitimacy of emails (for example, you're no longer right down the hall from your CEO who requested an unusual wire transfer), you may be unfamiliar with policies and procedures as they pertain to a work from home environment, and the list goes on.

We've developed a list of guidelines and tips to assist you as you prepare to work from home in a safe, functional work environment. Note, this list is intended for guidance and information purposes only. If you have any questions regarding these tips, please reach out to your supervisor or IT provider for additional information.

Guidelines & Tips

- Secure workspace
    - Ensure you can lock your devices (laptop, PC, etc.) and any business relevant information when not in use. Cable locks for laptops should be used when necessary. Laptops and devices should be locked out of sight and/or in the trunk if it must be left in a vehicle unattended
    - Avoid using your personal devices for work-related business
    - Safely perform conversations without visitors eavesdropping or shoulder surfing, especially while working in a mobile setting, such as a coffee shop
    - Protect the data you are accessing by using a VPN to log into the company network, and ensure you are protecting data visible on your screen with a screen protector. This is especially critical for employees who are required to be HIPAA compliant, PCI compliant, etc.
    - Restrict the use of devices containing business-relevant information. Do not let family members, friends, or anyone but yourself use company-owned devices or personal devices used for business purposes
    - Use strong unique passwords on all your devices and accounts to prevent unauthorized access
- Wireless Security
    - Change default Wi-Fi Router passwords
    - Enable WPA-2 or higher encryption
    - Ensure your local router firmware is up to date

- Limit the use of public Wi-Fi. Always use a VPN when connecting to public Wi-Fi. Never use public Wi-Fi to send sensitive information without a VPN
- Ensure all personal devices are secure with company-provided or personally owned antivirus and antimalware software company
- Updated IOT Device firmware (smart thermostats, surveillance cameras, etc.)
- Ensure default passwords are changed
- Ensure the software on all devices within your home network is kept up to date (corporate laptop, IOT devices such as cameras and smart thermostats, personal laptops/tablets, etc.)
- Review and follow corporate Bring Your Own Device (BYOD) and other relevant policies and procedures

AWARENESS

- Remote Work Employee Awareness
  - Be extremely cautious of email phishing scams
  - Limit social media use
  - Don't reveal business itineraries, corporate info, daily routines, etc.