Stimulus
TECHNOLOGIES

855-564-3166 P
702-952-2062 F
StimulusTech.com

6100 Mountain Vista St.
Suite 100
Henderson, NV 89014

Working Remotely: Best Practices

The ability to work from anywhere can be a great asset. It can keep your business up and running when employees aren't able to leave their homes; in a natural disaster or in an unprecedented occurrence like the current outbreak of the Covid-19 virus, which has millions of people at home in an effort to slow the spread.

Note: We can help with your transition to remote work. If you need assistance with this, give us a call or use the Contact Us form and we'll be happy to discuss your needs.
When remote work is necessary, it's important to understand the security risks to your business so you can take the necessary steps to help prevent breaches, loss of data, and compromises to sensitive information.

There are some basic guidelines to keep in mind and follow when working remotely:

Establish a secure workspace

- Be sure devices can be locked and not accessible by anyone else when not in use. Also, be sure any physical files and paperwork are securely locked away in a file cabinet or drawer.
- Don't use personal devices for work-related business. Only uses company-issued laptops, tablets, etc.
- Be sure phone conversations and online meetings are in a private space.
- 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.
- Only employees should be accessing the work device; family members and friends should not access the work computer
- Use strong passwords for all devices and accounts.

Secure WiFi

- Don't use default router passwords. Make sure you have changed the default password for your router to a strong, unique password only you know.
- Enable WPA-2 or higher encryption.
- Make sure your router firmware is up to date and continue making any new updates.
- Don't use public WiFi for your work-device or any work-related activity. If you are in a public place, be sure to connect using a VPN.

855-564-3166 P
702-952-2062 F
StimulusTech.com
6100 Mountain Vista St.
Suite 100
Henderson, NV 89014

Security

- Make sure all devices are secured with anti-virus and anti-malware software. Work devices should be secured with company-provided software.

IoT (Internet of Things) Security

- Make sure all smart devices have updated passwords and are not using the default password.

Do Your Updates

- All mobile devices, laptops, smart devices, and anything connected to your network should be kept up to date. Devices that are not up to date are more susceptible to cyber security threats.

Review Your Company Policy

- Business owners should have a remote-work and BYOD (Bring Your Own Device) policy. Employees should agree to and review policy as needed.

Awareness

- Anyone working from home should make sure they are taking the same precautions to protect against phishing attacks that they do at work. Check URL's, and verify transactions, especially if anything seems out of the ordinary.