Remote Work Checklist

HIGH POINT NETWORKS™

As IT professionals we've all had to adapt to a new way of doing business. HPN has worked with many companies to ensure that rapid changes to their IT environments do not lead to increase cyber-threats. Our security team is busy working with customers to identify vulnerabilities ahead of time, before they can have detrimental impact in the future.

We've developed a variety of security options that are budget conscious and fit any size business. Our mission, during this difficult time, is to keep your organization informed and protected. The best thing we can do is work together, keep a level head and not allow the bad actors to take advantage of stress and urgency. A good starting point for any business is to ask yourselves some important questions. Do you have a plan in place for the items on our Remote Work Checklist?

THINK ABOUT	RECOMMENDATIONS
How will you update your anti-virus and next generation anti-virus? ›	Make sure your anti-virus and next generation anti-virus can be updated remotely using cloud resources.
Is MFA in use? ›	Enable MFA for all applications that allow it. Pay specific attention to on-prem or cloud applications that store sensitive data.
Are users connecting securely back to office resources? ›	Enable VPN or other tunnels back to the office for secure access. This may require additional licenses and set up.
Do users have easy access to ask technology questions? ›	Make sure your users know who to contact for technical support and what hours that support will be available.
How will you remotely support your user's hardware and software needs? ›	Enable remote support services that are industry standard. Determine how you will securely log in to remote user's computers to support both hardware and software applications.

Remote Work Checklist

THINK ABOUT	RECOMMENDATIONS
Do your users know how to report a phishing email?	Phishing email attacks are increasing. Ensure your users know who and how to report a phishing email, especially if they have clicked through the email.
Have you restricted access to sensitive information?	Determine how, using network resources or VPN tunnels, you can restrict users to only the information they have in a typical working situation.
What secure conference solutions are you using?	Provide secure conference platforms so users are not using adhoc services to share company information. This may require additional licenses or set up. In addition, ensure that everyone has the ability and knowledge to create a remote meeting.
Are firewalls in place?	Ensure logins to your company firewalls are restricted to specific people or IP addresses. Assist remote users in setting up firewalls on their devices that will connect to the corporate network.
How will you handle patching devices?	Windows patches are delivered through Windows updates. Determine how your computers in remote environments will get Windows updates. Third party solution updates are often more difficult to apply remotely. Determine the risk of not updating those applications and how long you are willing to take that risk. Determine if local administrator access is necessary for updates and how to grant that temporary access to your remote users.
What is your DLP strategy?	Data loss prevention is a high priority with remote users. Educate your users on where it is appropriate to store sensitive information. Don't store company data on personal devices.
How will you provide unified communications?	Communicating with your customers is more important that ever. Soft clients for your communications require additional licenses and set up. If users can take their company provided phone home, create instructions for setting it up on a home network.
How much risk are you willing to accept if a non-managed device has access to your network?	If you can't control a device that is on your network, you can't control its level of anti-virus or patching status. This introduces a high level of risk to your network if the user is compromised. If possible, ensure devices that you don't control are segmented on your network.