SpartanTec
Incorporated

WORK FROM HOME
Remote Access Solutions

Secure Remote Access for Your Workforce

Executive Summary

Businesses large and small face a number of different potential emergency situations, such as illness, flood, hurricanes, and power outages. Organizations may not be capable of carrying on normal onsite business operations. SpartanTec's Remote Access Solutions support telework.

Business considerations when faced with the need to securely migrate traditional onsite staff to remote locations entail:

VPN and Endpoint Security: All users will need their laptops pre-loaded with their job specific applications. Each laptop should include a pre-configured client for VPN connectivity.

Multifactor Authentication: MFA is extremely helpful when trying to prevent cybercriminals from using stolen passwords to access networked resources. Remote staff should be provided a secure authentication token, which can be a physical device (ie. key fob), or software-based (ie. phone app), for connecting to the corporate VPN connection or logging into the network to provide an additional layer of identity validation.

Persistent Connectivity: A reliable and secure tunnel that has pre-configured wireless access points to ensure connectivity from remote user's location to corporate. For added security, a wireless access point combined with a desktop-based next-generation firewall will enable continual connections, advanced admission control, and a full spectrum of advanced security services, including Data Loss Prevention.

This report explains in plain, non-technical terms best practices for setting up remote access for you and your staff, as well as important questions you should consider to avoid making potentially costly mistakes.

Common Myths, Mistakes, and Misconceptions About Allowing Staff to Work Remotely

One of the biggest fears many business owners have about allowing people to work from home is the loss of control they have over that person. They believe that without someone standing over them, employees will goof off during work hours and become LESS productive.

But the hard results prove very different…

Working remotely ("Telecommuting") has grown at a steady 3% per year for more than 15 years. Prior to COVID-19 more than **23 million people were working from home** at least one day a week. The increase in telecommuting programs is no accident – it really IS working.

Admittedly, original telecommuting experiments were "do-gooder" projects focused on being earth friendly and generating business savings by reducing use of office space. Businesses started enjoying drastically improved turnover and productivity.

Take the Los Angles Bank for example; they decided to test telecommuting to see if it would help their 33% turnover rate. Here are the results…

> The experiment worked and within a year the turnover rate was cut to nearly zero and to everyone's surprise productivity went up 18% saving the regional bank more than $3 million dollars per year.

Since then there have been numerous, well documented, program studies reflecting promising results. AT&T allowed employees to telecommute on a regular basis from home in a New Jersey office of 600 people.

> Over a 5-year period a region of AT&T saved more than $11 million annually. Half the savings came from real estate savings while the other came from a measured increase in incremental work hours from employees who were able to have a higher level of concentration with fewer interruptions.

Small businesses think they cannot relate, **"But I don't have 600 employees…how does this apply to me?"** Regardless of the size of your business or your real estate situation, there are cost savings. For instance:

> On average, small businesses report saving $85,000 to $93,000 per year in lower turnover, reduced operating costs (gas, utilities, office space) and increased productivity after implementing teleworking programs. (Source: International Teleworking Advocacy Group)

There is no "one size fits all" solution; the best solution is greatly dependent on your specific business needs, the applications you use, how many people will be accessing your systems remotely, the available equipment and dozens of other factors.

Your IT provider should meet the following criteria:

1. **Remote Access Setup Experience**

   We have many years of collective experience setting up remote systems for our clients. It is far less expensive to use a trusted IT professional with experience and references to back them up than to hire someone at a lower price tag, only to have to spend more money to correct problems created by novices. Let us handle it for you and get it done correctly the first time with experienced technicians.

2. **Conduct a THOROUGH evaluation up front**

   If your provider doesn't insist on doing a thorough evaluation BEFORE handing you a proposal, do NOT hire them! If they don't do their homework they could easily sell you the wrong solution, causing you to have to spend MORE money, MORE time, and have MORE frustration getting to what you really need. Most consultants will do a quick, cursory review and provide a free recommendation (proposal) because they want to close the deal fast. Here is a short list of the things they should investigate or ask you:

   - What are your overall goals and specific objectives for allowing your employees to work from home or on the road?
   - How many employees will be working remotely? Will they be accessing the network at the same time or at different times?
   - What applications (including specialty or proprietary apps) and data will your employees need to access?
   - What type of devices will your staff use to access the network? (Laptops, Ipads, mobile phones, etc.)
   - What type of Internet connection will be available?
   - What levels of security do you want to have in place?
   - What level of monitoring do you require? Are there certain websites and content you want "off limits?"
   - Will the remote worker need to have the ability to print?

3. **You and your staff are trained.**

   So many IT service providers fall short on training. Perhaps they were great at installation but left you and your staff to figure out the technology they just sold you. Make sure your IT provider is capable and willing to do the "hand holding" required when installing any new process or technology.

4. **Make sure they INSIST on maintaining the network**

   Virtual office networks require more 'care and feeding' to make sure they work properly and stay secure. You cannot "set it and forget it" or you're asking for problems. Only hire an IT provider that performs consistent check-ups and updates of your network, under a maintenance or managed services plan.

5. **Make sure your IT services provider is willing and able to be a vendor liaison for your specific business applications or other specialty applications.**

   Critical applications may work fine within the office network but have issues that need to be worked out when accessed through a remote location. It's important to ensure your IT provider is able and willing to confirm your applications will operate efficiently remotely, which means they may need to get on the phone with the help desk of one or more of your software vendors. Some consultants do NOT offer this service or will charge you extra for it.

6. **Look for an IT provider that has expertise in setting up employee monitoring and content filtering.**

   It requires extra effort to protect company data when it's stored on a location outside of your office. Make sure the company you hire has expertise in setting up and managing content filtering and security for remote machines.

Not Sure If You Are Ready to Set Up Remote Access? Our Free Remote Access Consultation Will Help You Decide

We're currently offering a **Remote Access Consultation**. At no charge, we will review your current situation, business practices and needs and provide recommendations on how you can quickly and easily set up remote access for you and your staff.

We will also discuss your options, clarify any grey areas, and answer any questions you have, mapping out costs and steps involved so you know exactly what to expect.

You are under no obligation to do or buy anything; this is simply our way of demonstrating how we can make your remote access project a complete success.

Plus we'll give you a FREE "Home Office Action Pack" just for meeting with us! This package include:

- Home Office/Remote Office Checklist to help you verify the home or remote office is a safe and productive environment for the employee to work.

- Employee Agreement Template to outline the rules for your employees when working from home.
- Employee Equipment Issue Agreement to outline the rules of use and maintenance for any computer equipment, laptops, Ipads, cell phones, printers, etc. that are issued to the employee working remotely.

What To Do Now

To request your Free Remote Access Consultation and FREE Home Office Action Pack," do one of the following:

Call me directly at (843) 418-4792 or e-mail me @ lcarter@spartantec.com.

Best regards,

Lisa Carter
SpartanTec, Inc.
lcarter@spartantec.com
843.418.4792

