

Tips for Balancing Security and Productivity in Today's Work-From-Home Environment

Hackers are capitalizing on the global shift to working from home. A security-first approach keeps your employees productive and your company safe.

- Consider the core systems and critical applications that your staff uses. Are they on-premise or cloud based? Cloud services provide for desktop and application sharing that can maximize employee productivity onsite and offsite.
- Make sure employees have home access to common productivity applications such as Word, Excel, PowerPoint, etc., and that your licenses are adequate to cover all your needs. Also ensure employees' computers have solid security programs, such as Webroot or Sophos, and that their internet connections are solid.
- Evaluate your hardware needs, which may require purchasing more equipment than you had planned, such as firewall, laptops, mobile devices and printers.
- Protect connections with a virtual private network (VPN). Remote access software and VPNs can help provide employees secure access to corporate data.
- Train employees to identify phishing vulnerabilities, to never re-use credentials between accounts and to avoid using their personal computers or laptops for work-related tasks. Enhance security by implementing multi-factor authentication.
- Evaluate planned business travel and be sure your employees are educated about common "road warrior" risks, such as the use of public Wi-Fi.
- Unified communications, or the integration of instant and text messaging, voice, data, web conferencing and chat services are another option for maximizing productivity throughout your organization. Collaboration tools help keep your team connected in more ways than the technology.
- Review your bring-your-own-device (BYOD) policy. As more people use their own home computers, smartphones and tablets for business purposes, cybersecurity risks rise. With your corporate apps and data coexisting with personal apps and data you have an obligation to police both.
- In a crisis situation, how will you handle office phones, printers and other office infrastructure? Management should have a communication plan and roster of the cell phone numbers and home addresses of all employees.
- Update your business continuity plan to include a detailed strategy for operating in a remote workforce environment.

TeamLogic IT is ready to help you develop a remote workforce plan for your staff and operations. We can assist with staff training, home computer set ups and other services to help your business stay connected in the event of a local or national crisis.

Move forward with **The Color of Confidence**[®].