COMPUTER MAGIC
IT SIMPLIFIED

Checklist Remote Work

□ **High-Speed Internet:** Accessing and working in cloud-based systems, along with downloading and receiving needed files, will work best with a capable internet connection.

□ **Laptop or Desktop Computer with Windows 10:** Improved security, productivity, and support of applications like Office 365 and Teams will keep you efficient.

□ **Current Antivirus:** When you take work outside of the office, it's essential to remain protected against digital infections.

□ **Call Forwarding:** If your office is using VoIP calling technology, we can re-route calls that come to your business line to any device.

□ **A Headset:** We highly recommend using a headset for calls to improve the quality and ease of use.

□ **Webcam:** If you will be recording video or video calling/conferencing, a webcam is a must.

□ **Productivity Hardware:** Based on your needs, this could include multiple monitors, a physical mouse, and a keyboard for laptop users, a physical phone system, and a scanner. Think about what you use daily, and what would make your life more challenging if it wasn't available.

□ **Cloud Data & Collaboration Software:** Products like OneDrive, Dropbox, and Teams make working with a remote team easy and efficient. Ensure that you'll be able to easily share, manage, and collaborate on work with your team from anywhere.

What We Do Best

Efficient

Our experts will provide you with the results you expect. We apply speed without losing quality to protect your business.

Responsive

You'll never have to worry about not being able to reach us. We are available 24/7/365 days a year.

Affordable

We offer service plans that are within your budget. No surprise fees or contracts.

Get in touch

101 Nichols Road,
Monona, WI 53716

(608) 291-9723

tom@computermagic.us

www.computermagic.us

Remote Security Tools

Check these items off your list to confirm you and your team are set up to work from anywhere without compromising security or productivity:

□ Is multi-factor authentication (MFA) enabled? Did employees receive guidance on how to use MFA (and authenticator apps, if applicable)?

□ Is conditional access enabled and configured?

□ Do you have the ability to remotely wipe company data from lost or stolen laptops and mobile devices? Are you using whole disk encryption to encrypt the physical hard drive of company laptops?

□ Do you have an email security product in place? Were employees trained to recognize and report phishing attempts?

□ Have you installed a web security app to prevent users from visiting malicious sites?

□ Have you set up data loss prevention policies and set applicable restrictions on external file sharing?

□ Have you created a remote work and data protection policy for employees to sign?

□ Have you conducted end-user training on remote security policies and best practices? Do you have endpoint protection installed for all remote machines?

□ If you are subject to compliance regulations, do you have policies and procedures in place to ensure compliance? Are employees trained to enforce those policies?

What is your incident response plan during times of company-wide remote work?

Optional Security Tools

Virtual private network (VPN): A VPN provides an encrypted, private connection so employees can securely access company resources and applications from home or public networks.

Windows Virtual Desktop (WVD): WVD (Included with M365) enables central management and security of users' desktops by creating Windows 10 virtual desktops in Azure, allowing end-users to work remotely with a secure connection and securely store data in the cloud rather than on their local device. WVD separates the computer environment from user devices, significantly reducing the risk of confidential information on a personal device.

Next Gen Endpoint protection: The last line of defense against the newest forms of ransomware and malware.

Phishing prevention: Email is the top delivery mechanism for 96% of phishing attacks, so protect users with real-time anti-phishing technologies.

End-user security training: Make sure users are trained to spot phishing attempts and can recognize and report other common cyber threats.

DNS Filtering: Since remote workers don't have the protection of the company firewall, DNS filtering is needed to protect them from malicious and inappropriate websites.

Get in touch

101 Nichols Road,
Monona, WI 53716

(608) 291-9723

tom@computermagic.us

www.computermagic.us

Social