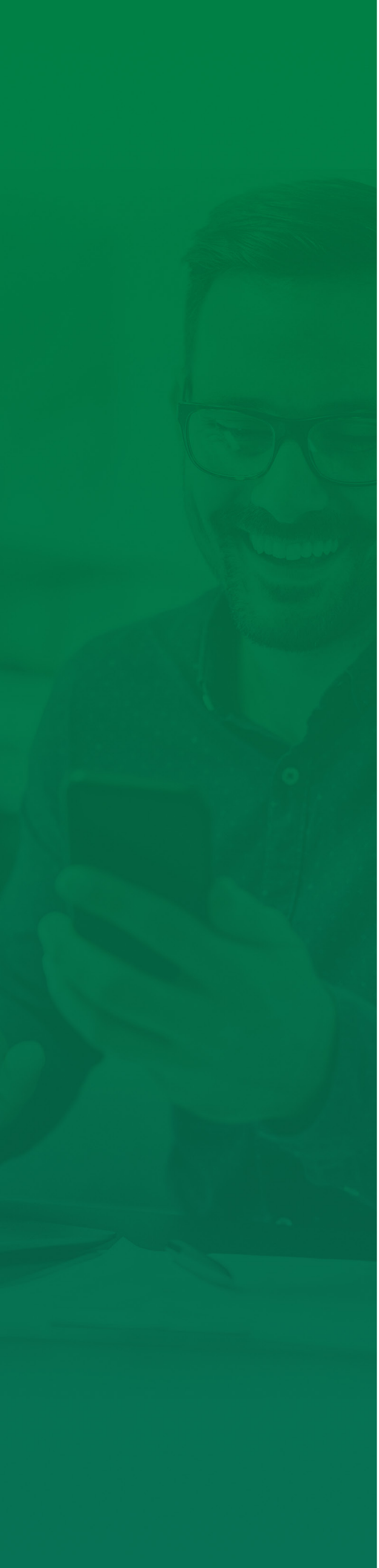
CSP

Your IT Partner

SECURING THE NEW NORMAL

A Business Owners Guide to
Productivity *and* Security

www.cspinc.com



CSP
Your IT Partner

ABOUT THIS GUIDE

This guide offers recommendations to help you adapt to remote work by optimizing your remote collaboration experience while ensuring you stay productive and secure.

Contents:

INTRODUCTION

Have you given any thought to the way your business will operate in a post-pandemic world?

According to 317 CFOs recently surveyed by Gartner, the business world may not change back when the pandemic is over — 74% of CFOs say they expect to move previously on-site employees remote post-COVID-19.

Regardless, once the pandemic has concluded, you'll be working in one of three potential scenarios:

Your entire staff returns to work in the office, requiring you to implement practices to maintain social distance and keep high-traffic and high-contact areas disinfected

Some of your staff returns to work in the office and some continue working remotely, requiring you to manage a hybrid IT environment

All of your staff continue to work remotely, requiring you to assess and improve the remote IT environment you've been using so far

The bottom line is that however you've managed remote work so far, if it's to be a part of your long-term vision for your organization, you need to make sure it's optimized and secure.

The rush to pivot to remote work at the start of the pandemic prioritized access to data with basic security measures. Now that the rush is over, it's time to implement more advanced and robust cybersecurity defenses.

THE PROS AND CONS OF REMOTE WORK

The remote work model offers a number of benefits that you've likely noticed over the course of the pandemic. Remote workers have seen the benefits as well:

77%

of remote employees say they're more productive when working from home

76%

of employees prefer to avoid their office completely when they need to concentrate on a project

98%

of remote workers want to continue to work remotely (at least some of the time) for the rest of their careers

However, for all the ways remote work is beneficial to both the organization and end-users, it's not without its challenges.

Ongoing Cybersecurity Considerations For Remote Work

When the COVID-19 crisis hit, it hit fast. Despite what may have seemed like a gradual build-up, it was virtually over the course of a single weekend in March that businesses across the US had to pivot to a remote work model.

Obviously, the first priority was maintaining business continuity. You needed to make sure your newly remote workers had the technology and the remote access necessary to do their work.

But the process doesn't end there - security is a complicated undertaking for remote work models.

In fact, 36% of organizations have dealt with a security incident due to an unsecured remote worker.

Continuing with a remote work model, whether entirely or in part, will require:

- Enhancing security measures
- Providing the right hardware for users working permanently from home
- Implementing more permanent file-sharing and collaboration tools

COMMUNICATION IN THE REMOTE WORKPLACE

The ability to communicate quickly and effectively with your team is a vital part of the modern working world, especially during the pandemic. In fact, among remote workers surveyed this year, trouble communicating is tied with loneliness as the most significant challenge they've encountered.

At this point in the COVID-19 pandemic, you should have a communication solution you rely on in place for your business, but that's not to say it can't be improved. You've likely had to incorporate a range of solutions, such as a video meeting platform, file sharing service, and more.

The bottom line is that communication and collaboration are foundational to productivity and continuity, whether you're in the office or not. Whether you and your team can communicate effectively while working from home comes down to the tools you have in place.

If you're not satisfied with your current communication methods, a primary consideration of yours should be the Microsoft 365 Ecosystem. It provides virtually every communication capability required by organizations operating remotely:

RECOMMENDED REMOTE SECURITY SOLUTIONS FOR HYBRID MODELS & LONG TERM REMOTE WORK

Even before the pandemic, it was becoming increasingly common for businesses to hire remote workers — that is, staff members that work from home, outside of the business' city of operation, and even much further away. It is important to recognize that when businesses start prioritizing remote access to data over the security of that data, they become an easy target for hackers.

Think of it this way — at the office, everything is protected by the same set of cybersecurity solutions — firewalls, antivirus software, etc. These are defenses that you've invested in and can trust.

Is the same true of your employees' home networks and personal devices? Probably not.

With so many employees operating remotely, working from a laptop or smartphone, how can you be sure that your data is completely secure? Are you taking the necessary steps to maintain security while your staff works from home?

Many owners and managers assume that a VPN is enough to protect their business while managing a remote work environment. That's not necessarily true — one wrong step, and a remote worker can put your network at risk.

Effective remote cybersecurity requires:

- **Two-Factor Authentication:** Two-factor authentication is a great way to add an extra layer of protection to the existing system and account logins. By requiring a second piece of information like a randomly-generated numerical code sent by text message, you're able to make sure that the person using the login credentials is actually who they say they are.

  However, this isn't just for websites and common user accounts — 2FA should also be enabled for VPN and Remote Desktops.

- **Conditional Access:** Conditional Access software gives you the ability to enforce controls on the access to apps in your environment, all based on specific conditions and managed from a central location. It's an extra layer of security that makes sure only the right people, under the right conditions, have access to business data.

- **Data Loss Prevention (DLP):** A DLP policy tracks sensitive data and where it's stored, determines who has the authorization to access it, and prevents the accidental sharing of sensitive information.

- **Hard Drive Encryption:** Encryption technology is a great way to protect important data. By making data unreadable to anyone who isn't supposed to have access to it, you can secure files stored on your systems, servers, and mobile devices, as well as files sent via email or through file-sharing services.

  This is especially important for remote devices, and employee-owned devices. Laptops and home-based hardware needs to be properly encrypted.

- **Backups:** Given that Microsoft 365 is a cloud-based platform, many users assume that their data is automatically backed up to a secure off-site location. But is that really the case?

  Reliable backup capability requires additional support. The key is in finding the right third-party backup solution to support your Microsoft 365 accounts. By adding data backup capabilities, you can make sure all your bases are covered.

PROMOTING PRODUCTIVITY AND SECURITY IN YOUR WORKING MODEL OF CHOICE

No matter how you plan to proceed, CSP, Inc. can guide you in both optimizing your IT environment to promote productivity, as well as in implementing the right cybersecurity standards and practices to keep your organization secure.

SCENARIO 1: All Staff On-Premise

- **Security:** Even though an all on-premise working model may be simpler than incorporating remote workers, you will still need a 2FA solution implemented for access to your email, Microsoft 365, VPN, and for any remote access to machines.
- **Productivity:** As you'll be operating in a conventional working environment, there won't be much of a change here, as opposed to a return to form. If you do need to provide access to data from outside the office (say, for team members on the road), Microsoft SharePoint and OneDrive are highly recommended.
- **Remote Access:** When needed, remote access should be secured by VPN and 2FA.

SCENARIO 2: Hybrid Remote & On-Premise

- **Security:** In a hybrid environment, you need to take extra care to make sure that both your on-premise staff and remote workers aren't putting business data at risk. That means securing all VPN connections, remote access to machines, and access to email and Microsoft 365 with a 2FA solution.
- **Productivity:** Maintaining productivity and communication between an in-office and remote staff is not necessarily easy - but Microsoft does provide a number of tools to help you do so. File storage and sharing can be handled through Microsoft SharePoint and OneDrive, Microsoft Teams offers a range of communication and collaboration capabilities.
- **Remote Access:** Using hot desks (multiple workers using a single physical work station or surface) can help to promote social distancing in the office, but you'll want to implement standards for disinfecting common spaces.

  In terms of remote access security, it's important for you to note that viruses can be transmitted from the remote user's devices over VPN. You will need to make sure any endpoints are configured to limit a VPN's ability to transmit dangerous malware.

SCENARIO 3: All Remote

- **Security:** In addition to the security standards laid out for the hybrid model (2FA applied to all access points), you will also need to consider whether you'll allow staff to use their own devices. Bring Your Own Device (BYOD) is a company policy that dictates how your employees use their personal devices for work purposes, prioritizing security above most other concerns.

  If you will allow BYOD for remote workers, you need to consider:

  - How to prevent that machine from putting your business data at risk
  - How to protect the user's private data on their personal device

- **Productivity:** As with the hybrid model, maintaining productivity and communication between an in-office and remote staff can be achieved with Microsoft SharePoint, OneDrive, and Teams.

- **Remote Access:** In an all-remote model, you'll want to consider moving all your data and line of business (LOB) applications into the cloud, which will eliminate your need for less secure and more complicated remote access to in-office machines.

  However, if you have LOB applications on your server currently, they will need to be migrated to the cloud, likely through Azure Hosting and used via Windows Virtual Desktops.

Remote Work Bundle Checklist

If you plan to make remote work a permanent part of your business' working model going forward, you'll want to be ready to onboard new employees quickly. Not everyone will have the necessary tools at home, and so, it's recommended that you have a number of remote work bundles ready to go:

- Laptop
- Monitor(s)
- Keyboard and mouse
- Phone system and headset
- AV Software

LEGAL, COMPLIANCE & HR CONSIDERATIONS

Please note that CSP, Inc. is not qualified to offer professional legal advice. However, we can recommend that you carefully consider data security and compliance when it comes to managing a partial or entirely remote workforce:

Make Sure You're Compliant: This may sound obvious, but that's not necessarily the case. Compliance means figuring out which legislation applies to you, what security vulnerabilities you may have been dealing with, and how to integrate compliance into your business processes.

- Determine which data compliance regulations you're subject to, and which ones may be in the works.
- Do what it takes to become familiar with the particulars of these systems – assign a small team to learn more about compliance.
- Develop a specific risk assessment checklist for compliance.

Make Sure You're Secure: Security and compliance are inseparable. Both are centered around protecting the integrity of your data. If you're not secure, then you're not compliant.

- Audit your IT to identify vulnerabilities that need to be addressed.
- Keep your hardware supported and your software patched.
- Confirm that your data "supply chain" and cloud partners (anyone else who stores or accesses the data for which you're responsible) are also secure.

Make Sure Your Staff Is Well Managed: The fact is that remote work doesn't come naturally to everyone. This new era of remote working has led to the types of issues that managers would have addressed directly in the workplace. It's not so easy now that you're cut off from your team members.

A recent study has found that newly remote workers across the country are encountering a series of challenges in their daily work life:

- **19%** experience loneliness
- **17%** have difficulty communicating and collaborating
- **8%** have trouble staying motivated

You can promote a more engaged and healthy remote workforce by following these tips:

- **Promote Accountability:** Try having your team share to-do lists with one another to promote accountability in their work. Have staff members pair up and meet on a regular basis to talk through what they've achieved, and how they can improve.

- **Set Firm Working Hours:** Your team may be working from home, but that doesn't mean they're on call 24/7 now. Make sure to set and follow working hours. Emails and items that come up in the evenings or early morning can and should be left until the start of the working day.

- **Make Sure They're Working In The Right Space:** Make sure that wherever your staff is going to work is comfortable, distraction-free, and as in-line with their normal workplace as possible. They may need to invest in an office chair, or even, depending on their work, a second monitor.

- **Promote Balance In Their Workday:** Make sure that your staff is striking the right balance at home. Just as they shouldn't be slacking off because they're not being supervised, they also shouldn't overwork themselves. Make sure everyone is taking breaks to decompress, stretch, stay hydrated, and relax.

- **Help Them Socialize:** Switching from a full office to their quiet house can be difficult for workers - don't forget to schedule time for business and casual communication. Your employees should still communicate on a regular basis with one another and with you.

NEED EXPERTISE GUIDANCE IN MANAGING A SUCCESSFUL AND SECURE REMOTE WORKFORCE?

If you plan to continue with remote work in one way or another, you may need to change your model of IT support — as you and the other C-level executives at your business have likely discovered since the start of the pandemic, your ability to work remotely depends directly on your IT support.

In the remote setting, technology is necessary so that you and your staff can:

- Access files, applications, and systems from a remote setting
- Collaborate with colleagues, partners, and customers via video conferencing solutions
- Stay secure against the increased rate of phishing attacks related to the pandemic
- Maintain communications with cloud-based phone systems that keep staff connected

CSP, Inc. can help — over the course of the pandemic, we've gained extensive experience in helping our partners to launch, optimize and secure remote work capabilities. Now that the mad rush to go remote is over, it's time to perfect your processes — and you don't have to do so alone.

Get in touch with the CSP, Inc. team today to get started.

CSP
Your IT Partner

(919) 424-2000 | www.cspinc.com | info@cspinc.com