Make remote working work for your business

Preparing your company for remote work and getting the most out of it

OKLAHOMA
TECHNOLOGY SOLUTIONS
SOLVING YOUR TECHNOLOGY PROBLEMS

TABLE OF CONTENTS

Why work remotely?

Your employees no longer have to be in the office to be productive. Thanks to technologies like the internet and the cloud, they can work remotely and accomplish their tasks anywhere, even on the go. And your business will only be better for it.

These are some of the ways your business will benefit from allowing remote work:

#1 Boost productivity

Let's face it: the office is not for everyone. For some people, creativity and the drive to work come more naturally in places that are quieter and where they feel comfortable. In fact, 76% of professionals think offices are full of distractions and 66% consider themselves more productive when they are away from the office.

And remote workers do deliver. A survey found that not only do they have less idle time than their in-office counterparts, they also work 16.8 more days in a year.

#2 Security risks

If you want to attract younger people to your team and tap into their knowledge of the latest trends and technologies, then implementing flexible working options is the way to go. Millennials, who will comprise 75% of the American workforce by 2025, consider flexible working options the third most important factor when evaluating job opportunities, behind work-life balance and opportunities for career advancement, respectively.

#3 Lower your operational costs

Office space doesn't come cheap, and the cost only rises further when you factor in utilities and upkeep. Allowing your staff to work out of the office helps you cut back on electricity costs. You can even save on office rent by having your entire staff work remotely full time.

#4 Make your employees happy

A study found that remote workers are happy with their job 22% more than those who never work remotely. They are also more willing to stay in their job longer and work above the regular 40-hour week compared to their on-site counterparts.

#5 Keep your workers safe

Flexible working options mean your employees do not have to risk their safety just to get to work. In case of a natural disaster or a pandemic, for instance, they can stay safe at home and still be productive.

How do you make remote working work?

Implementing flexible working options is not as simple as telling your staff to not come to the office. Your business needs to have policies and infrastructure that allow your employees to work as efficiently and securely anywhere, as if they were in front of their desks.

That said, it's not uncommon to encounter challenges when implementing a remote work policy, especially if your operations have been fully office-based for years. But as with any new endeavor, being as prepared as you can be is the key to making it work.

Below is a checklist of areas that require your focus and steps you need to take before implementing a remote work policy:

Organization

With some or all of your team's members working out of the office, how will you keep your business functioning optimally?

- [ ] **Determine who can and cannot work remotely.** For employees who can't, determine the reason and whether certain changes, such as providing a company laptop, will change their capability.

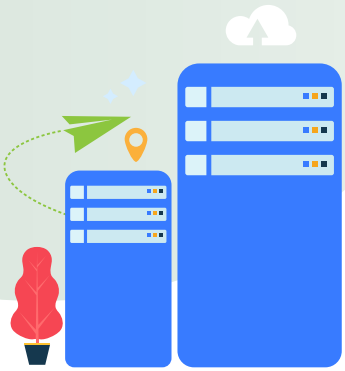
- [ ] **Research tools and applications.** Determine which ones you'll need to ensure smooth collaboration. For example, if you plan on holding meetings, video conferencing platforms like Zoom and Teams are a must.

- [ ] **Train your staff.** Get them familiar with tools, such as remote desktops and communication apps, that will be used for remote work. Also, train them on special procedures, such as turning in daily reports and completing trackers, that are necessary to ensure productivity and efficiency.

Security

How do you keep your business's data secure even when your employees are working out of your sight and reach?

- [ ] **Set up security guidelines.** Impose cybersecurity best practices, such as locking computers when they are unused and avoiding unsecured networks in public places, such as airports and coffee shops.
- [ ] **Implement a zero trust policy.** Set up your system to verify all users' identities whenever possible. Also, keep all users' access to information as minimal as is needed for them to complete their respective tasks.
- [ ] **Implement multifactor authentication (MFA).** Require users to input two or more authentication methods, such as biometric data, one-time passwords (OTPs), and personal identification numbers (PINs), before they can access the information they need. Microsoft says MFA helps prevent 99.9% of account compromise attacks.
- [ ] **Choose a virtual private network (VPN).** Get a business-grade VPN that will create a secure connection between your staff's and company's network. This will prevent hackers from eavesdropping and gaining access to sensitive information.
- [ ] **Install cybersecurity solutions.** Equip your staff's devices with business-grade cybersecurity tools like firewalls and anti-malware software to prevent hackers, malware, and other cyberthreats from penetrating your network.
- [ ] **Update all devices.** Keep the operating system (OS), apps, and cybersecurity tools on your staff's computers, smartphones, and other devices used for remote work updated to their latest version.
- [ ] **Educate your staff.** Increase your staff's awareness of common cyberthreats and make sure they know what to do during a cyberattack. For example, train your staff to identify telltale signs of phishing emails and what they can do to prevent these threats from harming your network.



Infrastructure

How should you prepare your current IT infrastructure to handle the possible impact of a remote work policy?

- [ ] **Ensure that you have enough bandwidth.** With people working outside, expect a surge of remote traffic to your network. Estimate how much bandwidth is needed to accommodate this influx of traffic and make sure your company has double of that, for good measure.
- [ ] **Make sure your VPN can accommodate multiple users.** Select a VPN that can accommodate multiple users simultaneously.
- [ ] **Confirm ready access to your cloud-based applications.** Make sure your staff can easily reach their remote desktop and other cloud-based applications even without having to connect to your company network.
- [ ] **Implement regular backups.** Set up your system to keep multiple copies of important files so your staff can keep working even when your primary services have slowed down because of high remote traffic. Regular backups also prevent downtimes caused by corrupted, stolen, or lost files.

Once you've cleared all the items on the list, what's left is to implement your remote work policy. Here are tips you should keep in mind:

#1 Do not micromanage
As the boss, you may feel compelled to ensure that your employees are making excellent use of their time, but inundating them with requests for updates won't do the trick. Keep in mind that one of the points of remote work is granting your staff autonomy to function in conditions that promote their creativity and productivity.

#2 Encourage transparency
That said, you do have the right to know what and how your employees are doing. Inquire about their concerns and ask for suggestions on how the remote work setup can be improved. You may require them to submit daily reports of the task they accomplished within the working day. Communication is crucial to your remote work policy's success, but don't overdo it.

#3 Be reachable
Provide your staff with an email address or phone number (or both) where they can reach you for information on work matters or to notify you of personal emergencies that might hinder them from working remotely. Make it a point to respond to their concerns or questions.

#4 Provide feedback
Call out employees who fail to follow your remote work guidelines, and give credit to those who do their best. Consistent feedback will help people take the provisions of your policy to heart.

What tools do you need for remote work?

Now that you have a good picture of what your remote work policy ought to look like, here are tools you need to make it work.

#1 Computer

You may allow your staff to use their own desktop or laptop computers. Alternatively, you may restrict them to using company-issued machines. Doing so could even be more secure, as you can demand that these computers be used for work purposes only.

In any case, computers used for remote work must be powerful enough to handle the type of tasks your employees do. Simple office work like researching on the internet, writing text documents, and making simple spreadsheets do not require too much computing power. For such tasks, these minimum specifications should be enough:

- Processor: Intel i3 or equivalent
- Memory: 4 GB
- Clock speed: 2.2 GHz
- Cores: 2
- Hard drive: 256 GB HDD

For much more demanding tasks like coding, crunching big data, processing images and videos, and creating multidimensional models, you'll need much higher minimum specs.

- Processor: Intel i7 or equivalent
- Memory: 16 GB
- Clock speed: 3.5 GHz
- Cores: 6
- Hard drive: 128 GB SSD

If you're choosing computers for your team, specs shouldn't be your only concern. In the first place, consider whether to issue a desktop or a laptop computer. The former can pack more power and is better suited for more demanding tasks, while the latter is portable and can be used virtually anywhere.

Lastly, consider price. Needless to say, newer and more powerful computers come with heftier price tags. Flashy units aren't always the best, though — select computers that strike a balance between cost and the ability to handle the tasks they will be used for.

#2 Cybersecurity tools

Never think of cybersecurity as just an option. Hackers will take advantage of any opportunity to steal your data, so you must be prepared for cyberthreats at all times, even when your employees are working outside the office. These tools are a must-have:

- **Anti-malware software** is designed to shield computers and mobile devices from different types of malicious programs, such as viruses, Trojans, worms, ransomware, adware, and spyware, among others. Firewalls filter out suspicious and harmful requests from your system while allowing trustworthy ones in. Together with anti-malware programs, firewalls are your basic protection against various cyberthreats.

- **Firewalls** filter out suspicious and harmful requests from your system while allowing trustworthy ones in. Together with anti-malware programs, firewalls are your basic protection against various cyberthreats.

Firewalls and antivirus software can be obtained for free. While these free versions suffice for casual users, the protection they offer against cyberthreats is hardly robust enough. Invest in full-version, business-grade cybersecurity solutions for the best results.

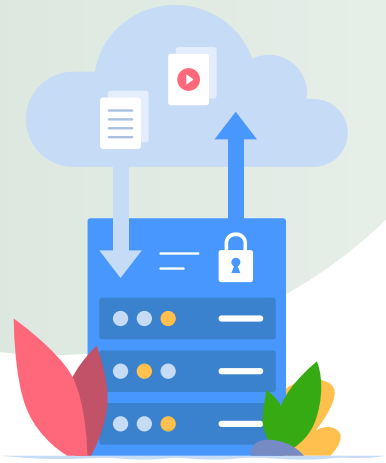
#3 VPN

Think of this: when your employees work remotely, the data they send and receive pass through multiple channels on the internet. This puts the data at risk of being stolen or eavesdropped on by hackers.

But when you use a VPN, it will provide a safe channel through which information can go directly to and from your business network away from the rest of the internet and its risks, effectively solving this problem.

Not all VPNs are created equal, though. Choose one that:

- **Doesn't keep logs** – The VPN must not store any of the data that passes through it in its servers. If it does, all the information must be deleted once your session ends. Check the VPN's terms of service (ToS) to learn how it handles your data.
- **Has strong security features** – Features to look for in your VPN include 256-bit AES encryption, protection from DNS leaks, and auto-connect functions. Also, make sure that the VPN is in a privacy-friendly country whose government will not snoop on your data.
- **Covers multiple devices** – Your employees will likely use not just their computers, but their mobile devices as well. Make sure your VPN supports mobile phones and tablets.
- **Has a large server network** – A sizable network means there is likely a server close to your location. The closer the server is, the shorter distance data has to travel and the faster your connection will be.
- **Runs fast** – If your business uses images, videos, and other heavy media, make sure your VPN is fast enough to handle large file sizes.



#4 Unified communications (UC) software

UC platforms allow you to integrate multiple communication channels into a single system. Imagine being able to access your emails, instant messages, phone calls, and others through a common interface. Voice over Internet Protocol (VoIP) systems, if you have them, also integrate with UC platforms.

The main benefit of UC is that it lets you and your staff communicate effectively anywhere and using any internet-capable device, even mobile phones. And because UC integrates with most customer relationship management (CRM) and other business applications, it grants you access to accurate, relevant data at all times.

#5 Cloud backup

Creating backups of your data is essential, whether you're working on-site or remotely. By regularly backing up your files, you:

- **Minimize the impact of data loss and corruption** – Should your files be corrupted or deleted accidentally, backups ensure that you don't lose them for good.
- **Prevent downtime from cyberattacks** – In case you fall victim to malware that deletes or blocks access to your files, backups allow you to restore your data and continue your operations even as you resolve the infection.
- **Ensure continuity after a disaster** – Backups prevent data loss resulting from disasters, allowing you to resume your operations at the soonest possible time.
- **Avoid penalties and possible lawsuits** – If you are in a highly regulated industry, such as healthcare, backups prevent the loss of sensitive data and the penalties that come with such an infraction.
- **Allow your staff to work anywhere** – Backups allow your staff to save their progress on their office computer and still continue working on the task in a different place at a later time.

Of the many ways to back up your data, cloud-based solutions are the most ideal for remote work. They are secure and accessible anywhere with an internet connection. What's more, they prevent your staff from depending on removable storage devices that can be easily misplaced or stolen.

#6 Collaboration and project management tools

True to their classification, collaboration tools like Slack and Skype make it easier for your staff to work on projects together. Functionalities include instant messaging, file sharing, voice communication, and even conference calls.

If you conduct regular meetings, you can do so remotely with specialized tools like Zoom and Microsoft Teams. They function well even with mobile data, which means your staff are not tied to places that offer free but risky public internet.

Project management tools like Asana, Trello, and Basecamp keep you and your staff aware of their tasks for any given period. What's more, these tools let you track everyone's progress in real time and even allow users to leave helpful comments.

Many of these tools have free versions, albeit with limited functionalities. Knowing the benefits they bring to the table, you should consider investing in their paid versions.

#7 Mobile tools

Smartphones and tablets are essentially miniature computers that your staff can use even for complicated tasks, depending on the apps they have. If you want to save money, you can have your employees use the mobile devices they already have, but with precautions to ensure your data's security.

Keep these tips in mind when designing your bring your own device (BYOD) policy:

- **Make passwords compulsory** – Demand that any device used for work be protected with a password to prevent third parties from gaining easy access to the files within.
- **Blacklist risky applications** – Media sharing and social networking apps are prone to being used to disseminate malware and other cyberthreats. Make sure devices used for work are not used to access these apps.
- **Train your staff** – You must educate your staff on the risks of human error and the telltale signs of malicious apps. Their training must also include the right response should they fall victim to mobile cyberattacks.

Make sure all mobile devices are equipped with business-grade VPN and cybersecurity tools. They must also be set up for regular data backups.

MAKE REMOTE WORKING WORK
FOR YOUR BUSINESS

How can Red Earth Systems help?

Whether you've had a remote work policy in place for a while or are developing one for the first time, getting the most benefit out of it is easier said than done. You need to plan well, implement the right measures, and carefully choose the tools you and your staff will use. And that's before you even get started working remotely.

At Red Earth Systems, our team of experts helps companies from your industry expand their borders beyond the corners of their office. Our years of experience have given us insights into which tools work for which industry and business needs. With our recommendations, you are assured of access to cost-effective and high-quality solutions that yield results.

Once you've implemented your remote work policy, our team can help you keep it functioning optimally. Our proactive services resolve any issue before it impacts your operations, so you can focus on running your business and improving your bottom line.

At Red Earth Systems, we make sure you are equipped to face the challenges of working remotely and reap the rewards that come with it.

Ready to start working remotely? Contact us today so we can get right down to business.

Phone: **405-622-5080** Email: **contact@oktechsol.com**

OKLAHOMA TECHNOLOGY SOLUTIONS
SOLVING YOUR TECHNOLOGY PROBLEMS

WWW.OKTECHSOL.COM