

REMOTE WORKFORCE CHECKLIST



10 Considerations for Creating a Remote Workforce Needs Checklist

What does your organization need to enable secure, reliable remote work options for your employees? Every organization is different, so it's difficult to create a one-size-fits-all checklist for what it takes to set your company up for remote work operations.

However, there are some general tools and functions that most remote employees will require. Use the following guide to help assess your needs and assemble a preliminary list of technologies and services for evaluation. Use this as a starting point for creating a more comprehensive list tailored to your organization's specific needs.

Even if you've already implemented work-from-home operations, the considerations noted here can help you identify potential gaps and opportunities for enhancing your current program and policies.

1. The Basics

If you don't already have remote work operations:

- Create remote work internal task force.
- Conduct employee surveys to assess remote work feasibility and sentiment.
- Define what kinds of remote work options will be available.
- Determine under which circumstances remote work will be permitted.

If you do have remote work operations underway:

- Conduct an employee survey to gather opinions on its success and suggestions for enhancing it.
- Conduct a survey with managers to gauge their thoughts on their employees' productivity, any issues that need to be dealt with and suggestions they have for improvements.
- Review the remaining items in this document, assessing how your current remote work operations are doing and where there may be gaps or areas that need improvement.

2. Computers / Mobile Devices

Most, if not all, your employees will likely need a computer or other device to perform their jobs and stay in contact with their colleagues.

Determine what devices employees need. That may include any or all the following:

- Laptop
- Tablet
- Smartphone
- Desktop computer
- Other (list) _____

Determine whether those devices will be/are:

- Company-owned and provided to employees
- Employees' own devices

Create or update policies that cover equipment security, maintenance, and other details related to equipment usage. Provide frequent training on the policies and keep them up to date.

- Policies
- Training

3. Network / Application Access

How will/do your employees access the applications, data and other tools needed to do their jobs? The capabilities, features, security requirements and advantages and disadvantages of the various options vary greatly – including by vendor, so it's important to carefully assess each one individually.

- Remote access/desktop sharing service
- Remote Desktop Service (RDS)
- Virtual Desktop Infrastructure (VDI)
- Desktops as a Service (DaaS)
- Workspace as a Service (WaaS, Virtual Workspace)
- Microsoft Remote Desktop or Apple Remote Desktop
- Direct access via Virtual Private Network (VPN). Usually, there are two choices when using VPNs:
 - IP Security (IPsec)
 - Secure Sockets Layer (SSL)
- Conditional access via unified endpoint management (UEM) tools
- Identity and access management (IAM)/Privileged access management (PAM)
- Secure access service edge (SASE)
- Software-defined perimeter (SDP)
- Software-defined wide area networks
- Zero-trust network access (ZTNA)

4. Business Apps

What apps are required for your employees to do their jobs currently? Survey employees and their managers. Compare the list against that IT has approved for use. This will help uncover any software in use due to shadow IT. Commonly used apps include:

- Accounting/Finance: Expensify, FreshBooks, QuickBooks, Wave,
- Architecture/Engineering: 3D StudioMax, AutoCAD, ARCHICAD, Revit, Rhino, Sap2000SketchUp, SolidWorks
- Collaboration: Bit.ai, Dropbox Paper Google Workspace,
- Communication: GoToMeeting, Mattermost, Microsoft Teams, Rocket.chat, Skype, Slack
- Customer Relationship Management: Belly, Nimble, Salesforce, Spendgo
- Digital workspace (project management, task management, instant messaging, cloud storage etc for working together without disruptions, even when they are physically present in the same office): Microsoft Teams, Kissflow
- General Office: Google G Suite, Microsoft 365
- Graphic Design: Adobe Creative Suite, CorelDraw
- Inventory Management: Delivrd, Sortly, SOS Inventory,
- Note Taking: Microsoft OneNote (Office 365 suite), Evernote, Notion
- Point of Sale (POS) and Payments: GoPayment, PayPal Here, QuickBooks, Square
- Project Management: Asana, Basecamp, Evernote, Jira, Teamwork, Trello,
- Screen Sharing/Recording: Join.me, Screenleap, TeamViewer,
- Time tracking/Team Management: Gusto, HotSchedules, Teamdeck,
- Video conferencing: Skype, WebEx, Whereby, Zoom
- Whiteboard: InVision Freehand, Miro, Sketchboard
- Other(s): _____

(The business apps listed are for illustrative purposes only. US Signal makes no recommendations as to preferred or required apps.)

5. Bandwidth

Internet bandwidth enables remote work, both on the remote employee side and the organization side.

- Set/review bandwidth requirements for employees' home internet services. A minimum of 50 to 100 Mbps download speeds is typically recommended, with at least 10 Mbps upload speeds if large files will be uploaded to the internet. This should be sufficient to cover the use of common business applications.
- Ensure your organization has sufficient bandwidth. Generally, you need about 10 to 15 Mb per employee. How many connected devices are on your network? You also need to think about is everyone's online activity. Things like email and web browsing don't take up a lot of bandwidth, but more complex activities — like video conferencing and streaming services — require faster speeds.

6. Data Backup and Recovery

Backup and recovery solutions are critical to mitigating data loss and corruption, even for remote employees. Depending on if employees are using their own equipment or company-supplied equipment, and how they're accessing company network resources, backup solutions may take the form of:

- Local backup and recovery processes. This may include employees backing up their data to an external drive and synchronizing data from that drive to file servers. Or employees may use FTP servers to transfer data from remote laptops to a data center.
- Remote backup and recovery tools, such as cloud-based backup
- In either case, you'll need to ensure you also have a tested disaster recovery plan in place in the event of natural or man-made disaster.

7. Network Security and Malware Protection

Cybersecurity is critical on both the employee and organization sides. Here are a few cybersecurity must-haves for any remote team:

- Antivirus, anti-malware, firewalls
- Employee monitoring software
- Endpoint detection and response (EDR)/Managed detection and response (MDR)
- Multi-Factor Authentication (MFA)
- Multi-point network backups
- Patch management
- Real-time security monitoring
- Vulnerability scanning

8. Cloud Storage

Cloud storage services enable remote workers to manage files, share data, and work more seamlessly as part of a distributed team. Make sure any storage option chosen follows all the necessary compliances while allowing employees to access important company data from any device or location. Common cloud storage services include:

- Google Drive
- Dropbox
- Microsoft OneDrive

9. Policies

Set policies for remote work to help ensure smoother operations. Keep in mind that not all roles can be done off site. Make this clear in your policies. Work with your Human Resources and Legal departments to ensure all policies are fair and meet legal standards. While policies must be adhered to, they also need to evolve to meet changing conditions or new information.

Among the areas that should be covered in your remote work policies:

- Eligible positions and employees
- Remote work expectations, including availability, responsiveness, communication frequency, and reporting
- Productivity and success measures
- Legal considerations, including for hourly remote employees
- Remote tools, equipment and supplies, such as what will be provided or how employees will be reimbursed for equipment that isn't provided; usage guidelines
- Technical support options
- Guidelines for setting up employee work environments
- Employee work environment technical requirements
- Security and privacy rules
- Required travel
- How compensation is handled for remote employees moving to a new city or state with a higher or lower cost of living.
- Consequences for rules violations

10. Cloud Infrastructure

It's likely that remote work operations will continue to grow, as more employees choose to work from home. The cloud can make it easier with benefits such as no infrastructure to purchase or maintain; flexible scalability; resources available on demand and priced based on only what is used; greater compliance; and built-in, high-level security.

Plus, the cloud allows for building a comprehensive IT stack that can serve multiple purposes in addition to supporting remote work operations, such as disaster recovery, compliance requirements, application development, storage and archival, and more.

If you're not already using the cloud, now is the time to consider doing so. Research the various options to determine what will work best for your organization's use cases:

- Public cloud
- Private cloud (on-site or third-party hosted)
- Hybrid scenario, entailing any combination of on-premises, colocation, private cloud and public cloud

Start Your List Now

It's likely there will be many other issues to consider in developing a checklist for creating or modifying remote work operations. It may be beneficial to work with a third-party company, such as a cloud services provider. These companies can help you determine what your organization needs — particularly in terms of technologies and infrastructure — to successfully offer and manage remote work options for your employees.

US Signal is among them. From assessments to virtual workplace solutions, US Signal can help you develop a solution that not only enables you to offer

secure, efficient remote work operations. We can create a solution that meets a full range of complex IT needs.



Sign up to get trial details!

www.ussignal.com/m/cloud-trial | info@ussignal.com | (866) 274.4625

