

Remote Workforce Checklist

Dos and Don'ts to Keeping Your Team Safe While Working at Home

As your workforce adapts to California's stay-at-home order while juggling homeschooling and cabin fever, your company is working to stay productive with a remote workforce. DiamondIT has developed this checklist to give you a head start.

FOSTER COMMUNICATION

Communication among team members and managers is always a priority, and with remote working, it is even more important.

Decide how employees will work together

- ✓ Use tools like Microsoft 365 and Microsoft Teams for collaboration and communication
- ✓ Designate a secure way to share files like Microsoft Teams and SharePoint
- ✓ Share expectations early and often for how to work remotely
- ✓ Take advantage of free trials: Try Teams for six months at no cost –

Call DiamondIT at (877) 716-8324 to get a Teams trial

Support your staff's use of technology

- ✓ Provide training for the technology your team will now use
- ✓ Support employees with helpdesk support they can directly access
- ✓ Send tips to employees to reduce frustrations with technology

PROVIDE SECURE TECH FOR YOUR TEAM

One of the biggest decisions you need to make is whether you will provide devices to remote workers or if they will use their personal devices.

Equip your employees with the tools they need

- ✓ Laptop or desktop computer with a monitor, keyboard and mouse
- ✓ Access to reliable, high-speed internet
- ✓ Remote access to company phones and voicemail
- ✓ A web camera for online meetings and presentations

Bolster your network security

- ✓ Set up secure network access for remote workers
- ✓ Review, revise and refresh antivirus protection and spam filters
- ✓ Use advanced threat protection layers including breach detection, crypto prevention and DNS filtering
- ✓ Deploy or update multifactor authentication policies and use
- ✓ Train employees on the latest pandemic-related cyberthreats and phishing attacks

TRAIN YOUR STAFF

Refresh remote workers' knowledge of policies, tools and security practices to keep this work-from-home experience productive and safe for your organization's employees and data.

Train remote workers to

- ✓ Use devices and other hardware at home
- ✓ Access software apps, features and systems they need
- ✓ Participate and initiate chats, calls and meetings
- ✓ Properly use a web camera
- ✓ Invite guests to meetings and manage recordings
- ✓ Spot phishing attempts and cyberthreats

Update and share technology-related policies

- ✓ Bring-Your-Own-Device policy
- ✓ Acceptable use policy
- ✓ Password management requirements
- ✓ Do not let family members or friends use company-owned devices
- ✓ Do not use public wi-fi to access your company network without using a secure, encrypted connection

KEEP YOUR TEAM ENGAGED

Regular communications will help to keep employees engaged in their work as well as head off any feelings of loneliness and isolation.

Check in regularly with your remote workers

- ✓ Make sure they have access to network information and tools
- ✓ Don't "check up" on remote workers, as it leads to disengagement
- ✓ Schedule regular one-on-one coaching calls and team meetings to keep everyone moving in the same direction
- ✓ Collect employee contact information such as cell phone numbers

Keep employees engaged

- ✓ Encourage nonwork-related communications to foster personal relationships and camaraderie
- ✓ Use direct messages and actions such as "liking" and posting emojis
- ✓ Publicly praise team members
- ✓ Pick up the phone and call your remote workers
- ✓ Use video during staff meetings