



Best Practices For Having Employees Work From Home

The coronavirus pandemic is forcing businesses to make tough decisions about how to maintain operations as they look to protect their staff and clients.

While some— such as grocery stores and medical facilities – will need to keep staff on site, and others are temporarily laying employees off, many businesses are allowing staff to work from home during these trying times.

While this can maintain a semblance of ‘business as usual’ it also comes with challenges and necessary precautions. Here are some tips suggested by a variety of experts:

- Ensure that employees have the tools they need to do their jobs remotely. Considerations should include whether they are allowed to take work devices home or if they will be allowed to use their home computers or smartphones. Let them know how to get any necessary office supplies and what records to keep.
- Make sure they know what they are expected to do from home and what hours they are expected to work. Make sure they know who to contact. Set up times for daily check-ins. Let them know how quickly they should respond to a work request.
- Have a communications plan. Do you have instant messaging, teleconferencing, or web-based video capabilities? Have you set up regular meeting times? What hours should employees or their supervisors be available? Who do they call with specific questions and when will those people be available? Ensure that employees and managers have a list of contact numbers and that they know how they should let clients contact them.
- Have a security plan. Do you have a VPN for secure access to your network? Have you stressed the need for strong passwords for computers and devices? Are computers and smartphones updated with the latest operating systems and software? Have you warned staff about possible email scams and reminded them not to open unsolicited email or to download attachments unless they are absolutely sure of the source? Have you told them to question all email, even if it looks official? Have you let them know that if they get email from top management or supervisors with out-of-the-ordinary requests to call the manager to confirm that request? Have you told them avoid the use of unsecure Wi-Fi networks? Are you allowing only as much access to systems as is needed based on each employee’s duties? Who should they contact if they are worried about a security breach? How should they back up and store their work?

- Let employees know about support options. Will they have technical support if they are having problems logging, completing tasks or if something is wrong with their device? Who will they contact and when can those people be contacted?

There is a lot to consider and decision-making time will be tight, but planning and clear policies will help your business and employees know what is expected.