Published on *The National Law Review* https://natlawreview.com

Remote Working: What Employers Need To Know

Article By:

Cory Rand

COVID-19 concerns have swept across the country in the last weeks. The Centers for Disease Control (CDC) and other governing bodies have called upon all Americans to do what they can to slow the transmission of the disease by practicing social distancing. For employers, that means seriously considering allowing their employees to work remotely.

For large corporations and tech companies, this may be an established practice. For many companies, especially those who haven't fully developed remote work policies and how to implement them, this may involve some immediate footwork to prepare and execute remote working capabilities. This inevitably involves addressing both logistical – and legal – issues.

Compliance Issues

Data Protection

Are you ready to have your employees handling work-related data from their homes? There are a range of data-security related compliance issues to be considered, especially for regulated industries like finance and healthcare.

Ideally, your business has policies in place for how staff should securely access, transmit, and store data. If you have a portion of your workforce that has worked remotely, it may even touch on this situation. If not, you'll need to consider what tools and resources to have in place that will allow workers to do their job effectively – and compliantly.

To ensure you've covered all your bases, make sure this policy is clearly distributed and communicated to all staff.

Data Breaches

Data breaches are an unfortunately common scenario in the United States. A typical user has a 27.9% chance of experiencing a data breach that could affect a minimum of 10000 records, and that's just in the course of personal use. For businesses, a data breach could have a devastating impact.

The risk of breach and liability exists whether it occurs on your business network or the home of a

staff member. In general, businesses are fundamentally responsible for protecting their data regardless of where workers are working. If employees are using their own computers, which may not be to the necessary security standards, you may be at additional risk. Employers must determine how to best protect the systems of their remote workers, even if it could mean providing anti-virus software or a VPN requirement for remote access.

Wages (Fair Labor and Standards Act)

Although many businesses are looking to transition large segments of their workforce to remote work, there may be limitations as to who can, or is permitted, to work remotely. Under the Fair Labor and Standards Act, remote work programs may conflict with requirements for fair payment for non-exempt workers who may be eligible for overtime in some situations. In these situations and grey areas, it's always better to err on the side of caution.

Capabilities

In addition to assessing the compliance needs of your remote working staff, you'll also want to consider the capabilities of your staff to handle their workload remotely.

Some questions to consider:

- What technology will your employees be using to do their job? Will they use their own computer? Will they access information from a smartphone? Or will you provide them for workers?
- What software is necessary and can it be accessed securely off your network? Will staff need to set up a Remote Desktop? A VPN?
- Will your workers have access to the internet? If so, is it a secure network or an unsecured public network?
- If information needs to be stored or printed, do workers have the capacity to securely do so from home?

Developing Guidance for Your Workforce

As you prepare to transition some or all of your workplace to remote work, it's imperative that you provide guidance and structure for your workers.

Things you can do to limit risks:

- Limit access to sensitive information by setting strictly controlled permissions on documents at the file or folder level.
- Investigate and recommend appropriate software to ensure security and productivity.
- Document and provide internal processes that offer clear instructions on practicing cyber safety at work, including setting up a secure network connection for remote work.

- Make sure your liability insurance is current.
- Commit to having a reliable IT presence available for staff in the early weeks of remote working.

There will be many questions in the weeks to come from your staff. One of the best things you can do for them is to provide communication and guidance. Although answers may take investigation and evaluation on your part, this guidance can provide much-needed security and continuity.

National Law Review, Volumess X, Number 77