California Employers Association™

FACT SHEET

Remote Worker Fact Sheet and Checklist

Remote work may be an option or, **in times of emergency,** a requirement. The following checklist contain some items to consider in order to create a remote work plan. Following the checklist is an article on remote work and security and trade secret/confidentiality concerns.

Essential vs. Non-Essential Personnel:

- □ Identify roles critical to business operations that cannot be done remotely
- □ Identify roles that require face-to-face customer interaction or direct and constant supervision and cannot be done remotely

Equipment and Technology:

- □ Inventory necessary equipment employees will need to perform job remotely (e.g. laptops, docking stations, monitors, phones, printers, office supplies).
- □ Assess adequacy of IT support to assist employees working remotely
- □ Address security, privacy and confidentiality concerns and protocols (See additional information at end of checklist)
- □ Evaluate communication platforms such as Zoom, Go To Meeting, Slack, Skype (See Managing Remote Work, below)

Preparedness:

- □ Have employees prepare in order to begin remote work at a moment's notice. For example, ask employees to bring home any necessary materials at the end of the day in case the need for remote work should arise (e.g., laptop, working documents)
- □ Take time now to digitize any relevant physical documents to make remote working easier
- □ If allowed, have employees screen shot any physical calendars, sticky notes, whiteboards or other physical documentation they may need.

Wage and Hour Issues:

- □ Consider all issues relating to non-exempt workers and remote work, including:
  - "After hours" work – set a daily schedule to avoid overtime issues and require pre-approval of overtime
  - Off-the-clock work – enforce timekeeping and no off-the-clock work policies
  - Meal and rest breaks must be taken. Managers need to confirm.
- □ Best technology for tracking time and productivity.
- □ Final pay is paid at employee's primary work location
  - If you terminate a remote employee, you must be prepared to deliver the final paycheck at the moment the employee is notified of the termination.

Reimbursement of Expenses:

- □ Reimbursement for reasonable and necessary expenditures and losses is required even if remote worker would have incurred anyway
  - Cell phones and plans
  - Laptop

    - Internet access
    - Other equipment, supplies and furniture
- Reimbursement options
    - Pay costs that allow employee to work at home to employers satisfaction (higher speed internet than employer needs paid by employee)
    - Allocate costs between business and personal use
    - Provide a remote work allowance (actual expenses over allowance still must be paid)
- Travel time to and from office for meetings generally paid

Managing Remote Work

There are a number of steps you can take to ensure that the remote work time (whether temporary or permanent) goes well for your workers and for your organization.

- Designated daily or weekly communication type and method
    - Communications platform that all workers will be required to participate in for group meetings. It could be thorough a phone conference, email, instant messaging, Slack, Go To Meeting, Zoom, and/or some other designated tool.
    - Create agendas for team meetings as well as minute meetings to help solidify communications.
- Have each manager explain their preferred method of communication. Don't rely too heavily on email or text. Call your employees or schedule video conferences.
- Provide clear goals, project deadlines and expectations.
- Provide feedback.
- Don't micromanage – if you don't do it while they are in the office, don't do it while remote. Track overall productivity and goals instead of minute by minute activity.
- Watch for overwork, as there is less of a clear boundary between work and home. Manage burnout and stress and use overtime policies requiring prior approval of overtime for non-exempt employees.
- Consider digital "social" time now and again – you can play a game at the end of the meeting, do some stretching, or send everyone a muffin basket before the morning meeting starts.

Checklist for a Remote Work Policy

Your policy should lay out the expectations you have for your workers. If this is a temporary situation necessitated by an emergency (such as a public health emergency or wildfires), additional considerations may apply such as whether work at home is *mandatory* vs. voluntary. CEA provides a Sample Remote Work Policy.

The following are some key elements of any remote work policy:

- Need to comply with all employer policies, practices and instructions.
- The work schedule and required times of availability, including meal and rest breaks (for non-exempt). Prohibit off-the-clock work and overtime without prior approval.
- Procedures and policy for checking in and best contact method.
- Participation in regularly scheduled meetings.
- How communication with staff will be handled.
- How meetings with customers, clients or other third-parties will be handled (and any restrictions on meeting size based on public health issues such as coronavirus).
- How expenses will be handled and any employee documentation requirements.
- Employer provided equipment and that employer maintains control of such property.
- Right to monitor equipment
- Security, privacy and confidentiality policies (see below article), including whether work can be done at a coffee shop for instance due to these concerns.
- Maintaining a safe work environment.

As COVID-19 Increases Remote Work, Cyberhygiene Is A Must

As the coronavirus continues to spread across the world, companies are now in full-scale preparation for potential disruptions to their business.

Some large employers, including Twitter Inc. and Amazon.com Inc., have already advised their employees to work from home if possible. Facebook Inc. has canceled its global marketing summit, and many other organizations have cancelled their attendance at businesses conferences as a precaution.

Even where employees are willing to fly internationally, travel bans may restrict their ability to do so. For many companies, one way — or perhaps the only way — to continue operations while protecting employees and their families is by permitting employees to work remotely. But doing so is not without its risks.

For any company that has information to protect — whether it is customer or employee personally identifying information, financial information, or confidential and proprietary trade secrets — allowing work-related data to travel home with or be remotely accessed by employees increases the risk that nonpublic data will find its way into the wrong hands. If that happens, it may result in significant liability or competitive harm to the company and may trigger a duty to report the data incident to consumers, regulators and/or business counterparts.

In short, cybercriminals will likely not take a corona holiday. While moving to a remote work arrangement under exigent circumstances is never ideal, there still is time to address the potential privacy and data security risks — and to develop clear guidance for employees to follow. These policies should be tailored to each company's specific risk profile and communicated clearly to all employees.

Although each company's information security defenses are unique, some of the most common risks to be addressed regarding remote work include the following.

Unsecure Personal and Public W-iFi Networks

Employees' home networks — and connected devices — many be vulnerable to malware or ransomware attacks through their wireless router. Hackers could monitor network traffic or access files that on connected devices. Employees may also use their personal computers on public networks at libraries or cafes, which are even less secure.

Companies should therefore strongly recommend that their employees secure their home Wi-Fi networks, which should be updated regularly, with a robust password, and, when possible, employees should not use computers containing sensitive information on public networks.

Working on Unsecure Personal Devices

Home computers may lack critical security updates that would otherwise protect their work computers. Additionally, these personal computers may not have screen saver timeouts, may not be password protected (or have weak or compromised passwords), and the hard drive may not be encrypted.

To the extent possible, employees should be advised to only conduct work on their employer-issued computers. Where this is not possible home computers should, to the greatest degree possible, be as secured as their business laptops and desktops.

Transferring Corporate Data Using Personal Email Accounts

Employees may send sensitive information to their personal email accounts, perhaps out of convenience to download on to a personal computer or print at home. However, many major email providers have suffered data breaches in recent years, and these accounts lack the robust protections that enterprise-grade accounts usually have, like multifactor authentication or logs that would help a forensic investigator determine the cause and scope of a breach.

Yahoo Inc. suffered several breaches that may have compromised the accounts of 3 billion users between 2013 and 2016. In addition to advising employees against sending sensitive company data to their personal email accounts, it is just as important to remind employees to permanently delete any corporate data remaining on their email accounts after they return to their normal working arrangement.

Subject to applicable law and corporate policies consented to by the employee, it may even be appropriate to monitor email systems to identify specific employees who have sent emails to their personal accounts and counsel them in connection with this poor practice.

Syncing with Personal Cloud Storage Accounts

similarly, employees may be tempted to use a personal cloud service account to transfer documents or data to and from office that may be less secure. Files may even be syncing from the employee's personal computer to the cloud without their knowledge. As with personal email, information security should monitor network activity, and employees should be advised to search these accounts for any work-related data on the personal cloud accounts and permanently delete it.

Physical Document Management and Destruction

Employees may take sensitive or confidential materials offsite that they would not otherwise. They may also print documents containing sensitive nonpublic information in public locations or on network printers with unsecure connections. Employees should be advised not to take critical materials off site unless unavoidable and never to print corporate documents at home (or in hotel business centers) unless absolutely necessary.

Additionally, employees without cross-cut shredders at home should be advised return all printed materials once they return to the office for proper destruction and to avoid disposing of documents at home or in a public place without proper cross-cut shredding.

Unsecure Connections to Employer Systems

In the absence of a secure virtual private network, employees may attempt to connect to a company's systems in an insecure manner, such as using remote desktop software to connect to their work computers.

To the extent you foresee a need to access information on a company's network — for example, many employees have a network-enabled personal drive to store their documents — investigate the viability of configuring a VPN for certain employees or for data that is critical for conducting business.

Remember also to require employees who have web access to corporate email to enable two-factor authentication to the web-accessible portal or any other web-accessible corporate network.

Unsecure Conference Call Lines

An increased need for conference call or video services may exceed the capacity of the company's existing accounts. A free or online-based service may seem like a sensible temporary alternative, but employees should be advised against using these for work-related calls without consulting with the company.

Some services may not be secure or may even record your employees' conversations by default. Employers are well advised to proactively work with your existing conference call provider to accommodate the temporary need or identify a secure alternative for employees to use.

Phishing Schemes and Other Fraud

Cybercriminals are always searching for security vulnerabilities to exploit, and many employ sophisticated attacks tailored to a specific company and its employees. A malicious hacker could target employees working from home by creating a fake coronavirus notice or phony request for charitable contributions.

The hacker might even go so far as to create a webpage that looks identical to the company's web-based platform to employee email and, impersonating someone in the information technology department, send an email to employees with a link to the imposter site in order to harvest usernames and passwords. Employees should be advised to look out for and report any suspicious communications.

Because many employees are justifiably concerned for the health and safety of themselves and their families, it is understandable that data security is not their top priority as they weather the coronavirus outbreak. However, with some careful planning, well-defined policies and transparent communication between employees and management, companies can maintain the security of their data while keeping their employees safe.

Article by *Joseph V. DeMarco, Partner at DeVore & DeMarco LLP and a mediator and arbitrator with FedArb.*

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.