LUQUE
www.luque.us

LOS ANGELES
7083 Hollywood Boulevard
Los Angeles, CA 90028

323.329.5410 T
917.924.2220 F

NEW YORK
25 Broadway, 9th Floor
New York, NY 10004

917.675.4910 T
917.924.2220 F

Best Practices for Your Working From Home Employees and Contractors: Protecting the Company's Confidential Information.

Now that all or virtually all of your eligible employees are working from home, and may be for weeks or months to come, it is important for businesses to remind employees of the importance of being extra vigilant now that they are working from home. Some "Work at Home" best practices for employees and contractors include:

i. Be extra vigilant in protecting company confidential information. If workers have reason to suspect that information is being stolen or disclosed, they should immediately inform management or their IT contact.

ii. Only address company business on company email accounts and, if possible, only on company provided equipment. Avoid the use of personal email, personal cloud storage, and social media for company related discourse.

iii. Employees should be the only ones with access to their computers, accounts, and related paperwork containing privileged work information. If possible, these should be locked away when not in use.

   - Information that can be protected as "trade secrets" will lose that protective status if the company can be shown to not have taken reasonable steps to protect it.

iv. Before discussing confidential matters in the home office, disconnect home assistant devices such as Google Home and Alexa. You never know when someone is listening.

v. To the extent workers need to print documents, instruct them not to throw the documents in the ordinary trash when done. Have them hold on to the documents until they can be returned to the office for proper filing or disposal.

vi. If possible, connect to the Office network through a VPN and/or require a two-factor authentication.

vii. Consider software that requires an email recipient to possess a designated digital signature to review email and open attachments. This will prevent the forwarding of confidential information to outsiders.

viii. Direct that all home computer screens be set to lock up after a few minutes of non-use and require passwords to unlock.

ix. Educate workers about malicious emails, SMS messages and other communications that appear to contain coronavirus related information, but actually contain malware designed to infiltrate your business's network. Only open messages from trusted sources and report any suspicious messages to a specific management or IT contact

Finally, also check with your vendors, suppliers, and outside professionals and ask them to advise you what measures they are taking with their work at home workforce to protect your business information.

While there is no "one size fits all" approach, each business should take some steps to at least remind at home workers of the importance of taking enhanced security measures from their home offices.