DINSMORE COMPLIANCE SERVICES

Dinsmore Compliance Services (DCS), an affiliate of Dinsmore & Shohl LLP, offers compliance solutions for investment managers and municipal advisers.

Cybersecurity and Privacy Concerns to Keep in Mind for Remote Work

As health concerns have increased due to COVID-19, many of you are transitioning some or all of your employees to a work-from-home situation. This creates various concerns regarding cybersecurity and data privacy. Below, we have outlined a number of different issues and steps you can take to ensure your and your clients' information remains secure during this time.

Digital Security

→ **Avoid Public WiFi.**

First and foremost, do not use public WiFi unless absolutely necessary when performing any work on your laptop. This is particularly important if any sensitive information will be accessed or transferred via email or other file-sharing methods.

→ **Cybersecurity Basics.**

Make sure you are keeping your security software up to date and turned on. Use passwords on all your devices and apps. Make sure the passwords are long, strong, and unique, which means using at least 12 characters and a mix of numbers, symbols, and capital and lowercase letters.

→ **Secure Your Home Network.**

This process starts with your router. Turn on encryption (WPA2 or WPA3). Encryption scrambles information sent over your network so outsiders can't read it. WPA2 and WPA3 are the most up-to-date encryption standards to protect information sent over a wireless network. If you do not see any WPA2 or WPA3 options, try updating your router software, then check again to see if WPA2 or WPA3 are available. If not, consider replacing your router. For more on this, read Securing Your Wireless Network and Secure Remote Access.

→ **Multi-Factor Authentication and Virtual Private Networks (VPNs).**

Using multi-factor authentication and a VPN is a vital step to take to strengthen your business' cybersecurity for employees who are now working remotely. If you are currently using these, ensure they are up to date and fully patched. **Before implementing these, speak with your business' cybersecurity expert to ensure you are using the right product for your business needs.** For more information, read Multi-Factor Authentication Guide and VPN Basics.

→ **Phishing Attacks and Email Security.**

Cyber criminals are taking advantage during this time and preying on the fears of the coronavirus by sending phishing emails that try to trick users into clicking bad links. Avoid clicking on links in unsolicited email and be wary of email attachments. If you were not expecting an email and it is asking you to click something or provide sensitive information, confirm the legitimacy of the email first with the sender, perhaps via phone or text. If you are sending any sensitive information over email, the data attached to the email should be encrypted.

DINSMORE COMPLIANCE SERVICES

Cybersecurity and Privacy Concerns to Keep in Mind for Remote Work

Physical Security

→ **Laptops and Home Computers.**

If you are using a laptop or other home PC, make sure it is password-protected and secure at all times. Do not leave it unattended, such as in a car, coffee shop, or public charging station. Also, if you are using a shared computer at home, ensure you have your own secure login, separate from other members of your household or roommates.

→ **Sensitive File Storage.**

If there is a need to transfer confidential information from your office to home, keep it out of sight and under lock and key. If you do not have a file cabinet, make sure you are using a secure room that can be locked.

→ **Disposing of Sensitive Documents and Data.**

This may seem obvious, but do not throw it in the trash or recycling bin. All documents containing sensitive or confidential information should be shredded. If this is not possible at home, keep the documents in a secure location until a shredder is available. Thieves know to look through trash for this type of information and will certainly be active during this time.

Other Privacy Concerns

→ **Recording Conference Calls.**

Many of the popular video conferencing apps, such as Skype and Zoom, offer video and audio recording capabilities. In their default setting, these apps will not automatically record your conversations. However, you should check your settings to make sure they are not set to automatic recording. As a general rule, you should avoid recording conversations unless there is a need to do so. Recording raises privacy concerns, particularly when mobile conferencing with a client. Some states require all parties to consent to a recording, while others only require one party. Although these apps alert everyone involved in a conference that they are being recorded, you should always get verbal consent before you begin recording a conversation.

→ **Mobile Conferencing Security.**

As many businesses move to mobile conferencing during this time, it is especially important to make sure communications both between co-workers and with clients is secure. Popular conferencing apps have an assortment of built-in security features and it is important that you check with your cybersecurity expert to ensure these features are enabled and up to date. Depending on what app you are using, there are additional optional security settings you should make yourself familiar with. One of the easiest and most common opt-in features you should be using is password protection. Recently, the widely used app, Zoom, was shown to be vulnerable to attacks without password protection. If you are using Zoom, read Zoom Security to help safeguard you and your clients' information.

→ **Smart Devices in the Home.**

Turn off smart devices, such as Alexa or Google Home, or work in a separate area of the house where smart devices cannot hear you.

→ **Reporting Exposure.**

When/if alerting employees to possible exposure, the most important rule is to not disclose the identity of the employee who has reported COVID-19 symptoms. This means not including the employee's name and also being extremely cautious not to disclose "anonymous" details that could be used to identify the individual. Furthermore, you should double-check your employee handbooks, employment contracts, and collective agreements to strictly adhere to any additional promises made regarding employee confidentiality and privacy.

Notifications of possible exposure resulting from the sickness of non-employees implicate different rules. For example, if the possible exposure is caused by a customer who has tested positive for COVID-19, you may have confidentiality obligations in the customer contract or privacy policy.

CONTACT

dinsmorecomplianceservices.com

Kevin Woodard
President
(513) 977-8646
kevin.woodard@dinsmorecomplianceservices.com

Jeff Chapman
Director of Client Relations
(513) 977-8647
jeff.chapman@dinsmorecomplianceservices.com