Seyfarth

COVID-19 & Remote Workforce:

Best Practices for Protecting Trade Secrets and Intellectual Capital

The coronavirus health care crisis is creating new issues for companies as huge sections of our economy are being forced to work from home. Enacting a remote work policy or expanding an existing policy to include remote work at all levels within an organization can have serious consequences for trade secrets and other confidential information

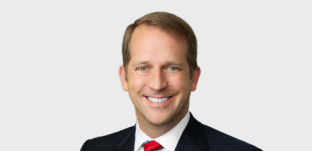
Working from home creates heightened risks of trade secret misappropriation or loss through:

- Unsecure personal and public Wi-Fi networks
- Unsecure personal devices
- Unsecure personal email accounts to transfer corporate data
- Syncing with unsecure personal cloud storage accounts
- Unsecure printed materials
- Unencrypted portable electronic storage devices
- Unsecure connections to employers systems (remove desktop software)
- Unsecure conference call lines
- Increased visibility in public locations of confidential information
- Increased phishing schemes and other fraud

This resource includes checklists to help you create the policies and electronic security necessary to protect your trade secrets during the pandemic. See the next page for checklists.

This material was summarized from a presentation by:

Michael Wexler
Partner
mwexler@seyfarth.com
(312) 460-5559



Jesse Coleman
Partner
jmcoleman@seyfarth.com
(713) 238-1805

Justin Beyer
Partner
jbeyer@seyfarth.com
(312) 460-5957

Using Policies and Communication to Create a Culture of Confidentiality

The pandemic highlights the importance of building a strong culture of confidentiality that ensures employees understand why and how trade secrets must continue to be protected, and providing practical proactive guidance with respect to:

- Protocols for secure teleconferencing
- Communication of out of office/off network status
- Policies for working on personal (employee-owned/non-company) devices
- Use of unsecure networks or less secure ones
- Best practices for use/dissemination of confidential information

Policy Checklist 1:
What Protections Do You Already Have In Place?

- ☐ Confidentiality agreements
- ☐ Return of materials agreements
- ☐ Invention assignment agreements
- ☐ Restrictive covenants agreements
- ☐ Do you have a social media policy that covers confidential information?
- ☐ Do you already have a bring-your-own-device policy? Different policies for different levels of employees? Does this need to be revamped or modified for the current situation?
- ☐ Employee handbook and information security policy—do you have these? Which applicable issues do they address? How do they align with mass work-from-home needs? Do certain provisions needs to be relaxed?

Policy Checklist 2:
What Should You Be Doing Now?

- ☐ Remind employees of these policies
- ☐ Hold a teleconference to address obligations (what is confidential, how to protect it)
- ☐ Even if you lack policies, be proactive
- ☐ Communicate expectations about device usage and best practices, including where they hold videoconference calls, best off-site work practices, how to protect information
- ☐ Send emails outlining company best practices (if no formal policy exists).
- ☐ Consider onboarding procedures
- ☐ Consider procedures for exit interviews and processes
- ☐ Consider the need for litigation, and keep in mind that civil litigation may be restricted or on hold

Bottom line: Don't let work-from-home environment erode/eliminate confidentiality efforts.

Protection: Electronic Security

Knowledge of current technology (and accompanying risks) and computer forensics is essential. Keep in mind the risks of a remote workforce: use of flash drives, personal email accounts, cell phone cameras, iPhones, portable music players.

Electronic Security Checklist 1:
What Should You Be Doing Now?

- ☐ Determine if you have a policy or procedures in place; if not, create one
- ☐ Audit/survey your employees: What devices or tools are employees using? Where are they working?
- ☐ Deploy company-owned devices and memory tools
- ☐ Sign-in screens are critical—make any needed changes now
- ☐ Issue reminder memorandum to all employees and conduct training call or webinar
- ☐ Enforce policies
- ☐ Track access to company data and files
- ☐ Use proper software to prevent malware, phishing, and viruses in email and attachments, and conduct training
- ☐ Develop plan now for return to normal work patterns and new remote workforce displacement
- ☐ Develop plan to ensure return of company information after shelter-in-place ceases.
- ☐ For laid-off/furloughed employees, copy hard drive and store, turn off access, conduct an exit interview, obtain a signed certification, issue a reminder letter, and monitor for issues

Electronic Security Checklist 2:
Protecting Trade Secrets from Cyber Security Threats

- ☐ Require all employee devices to be equipped with the employer-provided security software and the latest manufacturer software updates prior to permitting access to any remote systems
- ☐ Require multifactor authentication upon each login to a company portal
- ☐ Only allow remote access through a virtual private network (VPN) with strong end-to-end encryption
- ☐ Prohibit working from public places, such as coffee shops or on public transportation, where third parties can view screens and printed documents
- ☐ Prohibit use of public Wi-Fi, and require the use of secure, password-protected home Wi-Fi or hotspots
- ☐ Impose additional credentialing with respect to the ability to download certain sensitive data

Bottom line: Failure to install extra levels of security may be used by courts as an indication of a company's failure to take reasonable measures to maintain secrecy.