Trade Secret Protection With A Remote Workforce: 7 Practical Considerations for Employers

Insights
1.14.21

The COVID-19 remote work era is now in its tenth month, and employees continue to work away from the physical office, without in-person supervision, and perhaps outside of the company network. During this time, many employees have been adopting new practices for performing their jobs remotely and these practices can create new and increased threats to the protection of company trade secrets. For example, remote employees may be:

- Saving company information to personal devices;
- Sharing devices that are used for work purposes with other individuals in their home;
- Sending company information to personal email addresses;
- Printing documents at home;
- Using unsecured personal networks and devices; and
- Substituting in-person meetings with Zoom calls and increased email usage.

While these practices can be more convenient and can increase employee productivity, they can also increase the likelihood of company information being misused, exposed, and misappropriated. As employers embark on a new year, this may be the appropriate time to assess the steps being taken to protect their trade secrets.

So, what can you do to protect your trade secrets with a remote workforce?

1. Confidentiality Agreements

Determine whether your company has confidentiality agreements in place with its employees. If not, determine under relevant law whether and how you can obtain confidentiality agreements from your current employees. For example, some states require employers to offer something beyond continued employment in exchange for a confidentiality agreement from an existing employee.

2. Review And Update Company Policies

Review existing policies and make any necessary updates to address issues that arise in the remote workplace. For example, you can update company policies to address the need for employees to

review and discuss company information in an isolated, private setting. With remote employees sharing their workspace with others in the household, employees may not be as cognizant of their surroundings and may be less discreet with company information.

If your company implements a "clean desk" policy in the physical office, consider requiring your employees to abide by the same policy in their remote office. This can increase the likelihood that company information is not being left unattended in an employee's home, where it can be viewed by others, misplaced, or discarded.

Whether new policies are implemented or existing policies are maintained, you should ensure that employees receive notice of company policies and confirm their receipt and understanding of the policies.

3. Ongoing Training

Train your employees on best practices for protecting trade secrets while they are working remotely. You can provide training in a number of ways, such as:

Training videos that require employees to answer questions and achieve a passing score at the conclusion of the video;

- Remote training seminars; and
- Phishing email drills where the company tests employees to ensure that they can identify malicious emails.

You can also offer specialized management training to ensure that managers can properly educate employees on trade secret protection and to ensure that policies are being properly implemented and enforced.

4. Restrict Access

Ensure that company trade secrets are accessible to only those necessary even in a remote setting. You can review the remote access infrastructure to ensure that no loopholes exist that enable employees to access documents and information remotely that they would be restricted from accessing if they were in the physical office.

Given the increased use of Zoom meetings, you should also be mindful of protecting company information in this context as well. You should consider restricting participant access to Zoom meetings where confidential information is discussed, ensuring that meetings are password-protected, and using the "Waiting Room" feature.

5. Password Protection

In the physical office setting, companies routinely require employees to use passwords to access their workstations. However, given the nature of the remote workforce and the frequent use of personal devices for work purposes, you can consider the following:

Requiring employees to have passwords on all devices that are used to access company information;

- Using a third-party, password-protected application for accessing emails from phones and tablets; and
- Requiring passwords for logging into the company network and for accessing specific drives and documents on the network.

Employees should be required to change their passwords at regular intervals to increase the level of protection.

6. **Restrictions On Personal Devices And Personal Email**

Ensure that you have necessary safeguards to restrict information from being saved to personal devices. With employees working remotely, an employer would not want highly confidential information left unprotected on an employee's family computer. If employees must save information to personal devices, ensure that it is done only when necessary.

Likewise, ensure that you have necessary safeguards to restrict employees from sending company information to personal email addresses. In a remote setting, employees may be inclined to send information to a personal email so that they can print it from home or review it on a personal tablet. Not only could this result in a trade secret taking hard-copy form or a trade secret being stored on a personal device, but it also leaves the information unsecured in the employee's personal email account.

7. Secure Destruction Of Information

For employees who must have hard-copy materials when working remotely, instruct them to store the materials in a secure place and take steps to ensure that they are securely destroyed when the materials are no longer needed. Similarly, if an employee must save company information to a personal device or send it to a personal email account, take steps to ensure that the information is permanently purged when it is no longer needed.

If you have any questions regarding trade secret protection for your organization, please consult a Fisher Phillips attorney in the Employee Defections & Trade Secrets practice group.

Related People

Jeffrey M. Csercsevits
Partner
610.230.2159
Email

Service Focus

Employee Defection and Trade Secrets