Protecting Confidential Information and Trade Secrets from Defecting Employees

Publication
11.01.13

In today's business world, the entirety of a company's most significant information can be uploaded to a device the size of a thumbnail and taken by a departing employee. The consequences can be devastating. With advances in technology, it is more important than ever for companies to identify their confidential information and institute measures to preserve and protect that information from employees who decide to leave the company.

Use Technology to Control Information
As a first step, companies should consider which employees need access to what information. Once the determination is made, employers should require passwords to access any company computer, and use additional passwords to restrict employees who do not need to view more sensitive company information. Some companies are even employing voice-recognition software and more advanced methods of confirming identities before allowing access to more sensitive information. In addition, businesses can consider encrypting files and folders that they do not want easily accessed.

Companies that allow employees to access or store confidential information on their personal devices should particularly consider protecting information through technology. Higher-end controls may be needed for documents on remote computers or mobile devices, and companies may want to contemplate requiring software on laptops and smartphones that will enable the company to remotely wipe the proprietary contents of these devices as soon as the employee resigns.

Implement Agreements
Although a company can go a long way toward protecting its information through the use of software and other technology, these methods are not fullproof. Therefore, companies should also institute policies affirming that company information is confidential and must be treated as such. Companies should consider what types of information they deem confidential and proprietary, and describe that information in their confidentiality agreements. Since an increasing number of employees are re-creating information once they arrive at their new employer, the company should also specify that even information retained in memory is confidential and should not be used or disclosed other than to conduct business on behalf of the company.

Disseminate a Social Media Policy
Many companies encourage employees — particularly those involved in sales and marketing — to use social media sites to increase their contacts and communicate with customers. Yet, this social

use social media sites to increase their contacts and communicate with customers. Yet, this social interaction, which is very beneficial while the employee is working to promote the company's interests, can also be used to divert information and customers once the employee resigns.

Crafting a social media policy that will protect your company's confidential information and limit communications with customers will likely be one of the most important steps that the company takes to protect itself, as the Internet and social media redefine how companies do business.

Monitor Employees and Conduct Exit Interviews

If the company suspects that an employee might be planning to resign, it should not wait to begin monitoring her activities. By monitoring an employee before she departs, a company can learn about activities that may be harder to detect after she leaves.

The article appeared in Volume 28, Number 8 of the *The Corporate Counselor* in November 2013. Please click link to read entire article.

Attachments

46069_Nov13 Corp

Related People

Susan M. Guerette
Partner
610.230.2133
Email