



---

Portfolio Media, Inc. | 648 Broadway, Suite 200 | New York, NY 10012 | [www.law360.com](http://www.law360.com)  
Phone: +1 212 537 6331 | Fax: +1 212 537 6371 | [customerservice@portfoliomedia.com](mailto:customerservice@portfoliomedia.com)

---

## Protecting Trade Secrets When Employees Depart

*Law360, New York (September 18, 2009)* -- According to a recent survey conducted by the Ponemon Institute (a research group in Arizona), 59 percent of departing employees steal confidential information from their employers.

The survey, of nearly 1,000 persons who were laid off, fired or changed jobs in 2008, found: 53 percent of respondents downloaded information onto a CD or DVD, 42 percent downloaded information onto a USB drive and 38 percent sent attachments to a personal e-mail account.

Further, 82 percent of the respondents said their employers did not conduct a review of their paper or electronic documents in conjunction with their departure.

While there is no sure-fire way to prevent employees from taking data when departing, there are a number of practical steps that employers can take to reduce the likelihood that an employee will do so. By implementing these tips, an employer will also create a company culture where confidential information and trade secrets are taken seriously.

And, in the event that an employee steals information despite implementing these tips, the company will have positioned itself to demonstrate that it took all reasonable steps to prevent the misappropriation, thus increasing its odds of prevailing if it decides to pursue litigation against the former employee.

### **Establish a Confidentiality/Nondisclosure Policy**

Every employer should have a confidentiality policy prohibiting employees from disclosing or improperly using the company's confidential and trade secret information.

In general terms, a confidentiality/nondisclosure policy should: (1) identify the company's information that is considered confidential and trade secret (in a way that is meaningful and specific to the company's business); (2) prohibit unauthorized use or disclosure of the information; (3) set forth the consequences to the employee of

improper use or disclosure; and (4) require the return of all confidential and trade secret information at the end of the employee's employment.

A confidentiality policy can be part of an employee handbook, a separate policy, or a free-standing agreement. If it is a policy or part of an employee handbook, the employee should be required to sign an acknowledgment indicating that the employee has received and agrees to be bound by the policy.

### **Establish Specific “Protective” Policies/Protocols**

A company should also consider implementing a specific set of policies/protocols for protecting trade secrets and confidential information.

The policies should set forth the measures the company takes to protect trade secrets and confidential information. The goal should be to ensure that the measures are reasonable and enforceable, sufficient to be an effective deterrent, and withstand scrutiny in litigation.

There are several issues to consider in crafting protective policies, including:

Limiting access to confidential information and trade secrets. Employees should only have access to confidential information that is needed to perform their job duties.

#### *Limits on Physical Access*

This might include storing confidential information in a secure location protected by security measures (e.g., requiring electronic card keys, badges, and/or a check-in policy for visitors). An employer may also want to consider a “check out” system whereby access to its most important trade secrets is tracked at all times.

#### *Limits on Electronic Access*

There are a number of methods to limit electronic access, including requiring passwords to access certain company databases or systems, requiring passwords to be changed periodically, restricting certain segments of a company's computer network to certain employees, and “pop-up” warnings reminding employees of their confidentiality obligations each time certain systems or databases are accessed.

Employers may also want to consider prohibiting employees from using personal e-mail accounts to access confidential information.

#### *Identification of Confidential Documents*

An employer should consider regularly using restrictive legends such as “Confidential” or “For Internal Use Only” on documents that it deems confidential.

If an employer does decide to use such designations, it is important to train employees to use this designation consistently and in an appropriate manner. At the same time, it is important to not overuse the designation in order to avoid diluting its relevance.

#### *Access by Independent Contractors and Third Parties*

Employers who provide temporary access to confidential or trade secret documents to independent contractors or outside consultants should consider a policy for ensuring that those individuals also agree to the company's confidentiality policies.

#### *Securing Remote Access*

Employers who allow remote access by its employees should consider appropriate security measures to ensure that such remote access is not misused.

#### *Document Retention*

Employers should also consider how confidential documents are to be disposed of (e.g., shredding as opposed to simply throwing such documents in the trash).

#### *Electronic Monitoring of Employees*

Employers should also address electronic monitoring to ensure that employees understand and acknowledge that the company has the right to review their e-mail, Internet access, and computer use to check for misappropriation.

Doing so will prevent an employee from claiming that evidence obtained against them was obtained in a manner that violated their reasonable expectation of privacy.

### **Conduct Training on These Policies/Protocols**

Once policies/protocols for protecting trade secrets and confidential information are established, the next critical step is ensuring that the individuals responsible for enforcing these policies/protocols understand the policies and actually follow them.

Training personnel on these policies also conveys that the Company takes them seriously. Such training should occur at the outset of employment and periodically during employment.

### **Remind Employees of Their Confidentiality Obligations**

Employers should also periodically remind employees of their confidentiality obligations. This can be as simple as sending an e-mail or making an announcement at a company event or training.

Reminding employees of the importance of a company's trade secrets and confidential information helps to create a culture where such information is valued, and makes employees more likely to think twice before walking out the door with your information.

## **Conduct Exit Interviews**

An exit interview is a great opportunity to convey to a departing employee the seriousness with which the company treats confidential information and the expectations the company has of the employee going forward. An exit interview should include a review of the types of confidential information that cannot be taken.

If the employee has previously executed any agreements regarding treatment of confidential information, this is the time to remind the employee of those agreements, explain that the employee's obligations to protect the information are ongoing, and that the employee must also comply with any other ongoing restrictive covenants (such as covenants not to solicit employees or customers).

At this meeting, the employee should also be provided with a copy of any previously executed agreements.

An exit interview is also a great opportunity to get a sense of whether it appears the employee is inclined to take information, and thus whether further investigation is warranted.

In addition, employers should consider asking employees about where they plan to work. If an employee is not truthful and has taken confidential information, the company will be in a better position to obtain immediate equitable relief in court.

While exit interviews will obviously evolve during the course of the interview itself, they should be structured and include a check-list of topics to cover and questions to ask (e.g., "Do you have any company documents at home or in another location?"; "Have you returned all flash drives that contain company information?").

During the interview, employees should also be encouraged to ask any questions they may have.

## **Consider Requiring the Departing Employee to Sign an Affidavit/Certification**

Employers should also consider requiring their employees to sign an affidavit/certification stating that the employee has returned all data/property to the Company, and has not provided any data to anyone except in the usual and ordinary course of duties.

Requiring the employee to execute a certification emphasizes the importance of returning all data; if it later turns out that the employee took information and litigation ensues, the false certification can be used against the employee.

If a departing employee refuses to sign such a certification, it might suggest that further investigation is warranted.

### **Disable Access**

Once the employer is aware that an employee is leaving, steps should be put in place to limit or eliminate that employee's access to the company's trade secrets and confidential information. This might include changing passwords, requiring the return of laptop computers and handheld devices, and eliminating remote access.

### **Check for Signs of Misappropriation**

A departing employee's computer and e-mail should be reviewed to determine if the employee has recently engaged in any activity suggesting theft of information.

For example, has the employee recently sent a large number of files to a personal e-mail address, or copied a large amount of data from the company's system?

The extent of the necessary investigation will vary based on the circumstances, and can range from a quick e-mail review to a complete forensic review by an outside expert.

If an investigation involves interviews of other employees, be mindful that conversations and written communications not protected by the attorney-client privilege may be discoverable if litigation ensues.

An employer should also ensure that e-mails sent to the departing employee following the termination date are automatically forwarded to another company representative.

Not only is this important to provide for a seamless transition of duties, but it also may reveal further wrongdoing by the employee (e.g., an e-mail from a customer to the departing employee responding to a solicitation to transfer business to the departing employee's prospective employer).

Investigating each departing employee's computer use as a matter of course not only creates a culture where trade secrets and confidential information are taken seriously, but, in the event misappropriation of trade secret litigation arises with an employee, it demonstrates that the employer takes reasonable measures to protect its information.

### **Consider Follow-Up Letters**

Another option to consider is a follow-up letter to the employee and/or the new employer regarding the former employee's continuing obligation to protect your information.

A follow-up letter to an employee may make an employee reconsider a plan to use information wrongfully taken. It also demonstrates that you take reasonable steps to protect trade secrets.

Putting a new employer on notice regarding a former employee's continuing obligation is another option, and is typically reserved for situations where there is evidence to suggest that information has been taken or when the former employee had access to particularly sensitive information.

In such situations, a letter to the new employer may be sufficient to ensure that the new employer takes additional steps to guarantee that the former employee does not breach his continuing obligation.

If the new employer fails to take such precautions and the former employee subsequently uses trade secrets of his former employer, the new employer may become liable for the employee's actions under a theory of negligent or intentional interference with contractual relations, as well as trade secret misappropriation.

### **Preserve Evidence if it Looks Like Foul Play**

Lastly, if there is reason to believe that an employee has taken confidential information or trade secrets, the evidence of such misappropriation should be preserved.

This includes retaining any e-mails or other documents suggesting that an employee has acted improperly, and also creating a forensic image of the employee's hard drive.

Keep in mind that if litigation ensues, the company may need to demonstrate the chain of custody for such evidence.

While there is no way to ensure that a departing employee does not steal a company's confidential information or trade secrets, these tips will help create a culture where employees are less likely to do so, and also create a strong record demonstrating reasonable steps to protect your company's information in the event of litigation with a former employee for misappropriation of trade secrets.

--By Eric Amdursky (pictured) and Mark W. Robertson, O'Melveny & Myers LLP

*Eric Amdursky is a partner with O'Melveny & Myers in the firm's Silicon Valley office. Mark Robertson is a partner with the firm in the New York City office.*

*The opinions expressed are those of the authors and do not necessarily reflect the views of Portfolio Media, publisher of Law360.*