Best practices in hiring to protect trade secrets

Inside Counsel article by Margaret Keane and Rajiv Dharnidharka

Employee mobility is a boon to employers and employees alike, but it also presents unique challenges for preserving trade secret information. Those challenges include not only preserving one's own trade secrets on the back end, but also defending against accusations that an employee has misappropriated a former employer or third party's IP on the front end.

Rather than waiting for those challenges to ripen into costly litigation, employers should adopt four best practices on the front end – during the onboarding process – to prevent disputes from arising in the first place and – in the event they do arise – being prepared to defend the company. Those four best practices are:

Be particular about process

A strategic onboarding requires smart preparation. Employers should ensure that the right documents and processes – tailored to address anticipatable challenges – are in place long before onboarding begins. Together, those documents and processes should inform new employees of their responsibilities, erect a firewall between the employer's IP and that of third parties, and prevent disputes from arising between the employer and employee. Each of these goals is discussed in greater detail below.

Alert onboarding employees to third-party IP

The onboarding process should alert new employees to the fact that they may possess third-party trade secret information or other IP obtained while working for a former employer, and memorialize these issues and obligations in employment agreements and related documents executed prior to the new employee joining the company. That IP could be owned by the former employer, or by third parties who shared the IP with a former employer pursuant to a confidentiality agreement. Unless alerted, new employees may not be aware that they possess third-party IP, may not understand their duties to preserve the confidentiality of that information, or, sadly, may not grasp the severity of the consequences of violating these duties in following an "everyone else is doing it" mentality. A new employee who fails to understand those duties may use or disclose that information on the job, contaminating his or her employer's IP and exposing the employer to costly litigation. Defending a trade secret misappropriation lawsuit could cost an employer millions of dollars in legal fees alone.

To prevent actual or perceived misappropriation of third-party IP, employers should actively – not passively – educate onboarding employees about the variety of IP to which the employee may have been exposed during prior employment. Employers should consider that trade secrets may take wildly different forms in different industries or occupations. For example, engineers may have encountered trade secret circuit schematics, whereas sales professionals may have encountered trade secret customer lists. A new employee may not appreciate that a document or list used during prior employment is a trade secret owned by the former employer.

Keep out third-party IP

After alerting onboarding employees that they likely possess third-party IP, the employer should set out a clear policy to

prevent employees from using or disclosing that information in both a policy manual and an employment agreement. The policy's purpose should be to erect a firewall between the company's own IP and that of third parties. By doing so, the employer will not only mitigate against the chances of employees misappropriating others' trade secrets, but will also build a basis for defending against future accusations, if they arise.

The policy manual and employment agreement should be unequivocal and concise. With few exceptions, it should instruct each new employee to leave behind any documents, devices, or communications used or obtained during prior employment. It should prohibit the employee from using or disclosing third-party IP in any manner whatsoever. And, the employee should agree not to bring onto the premises of the company – or upload to company devices or systems – any unpublished or proprietary information belonging to a third party unless consented to in writing by the owner.

Define the employee's ownership rights

Employers should also anticipate and prevent future disputes between the employer and the employee. A common source of disagreement is ownership of information created by the employee prior to joining the company. Another is ownership of information created during the employee's time at the company. Onboarding documents – including the employment agreement and Proprietary Information and Information Assignment (PIIA) – should include separate written provisions on each topic.

A "prior inventions" provision should set out ownership of inventions and other information created before the employee joined the company. It should list every invention, original work of authorship, trade secret, and other intellectual property that the employee created in the past and which belong to the employee. If there are no such prior inventions, the employee should confirm as much. The provision may also address the possibility that prior inventions may be incorporated into the company's products. Consider adding a provision providing that, in that event, the employee grants the employer a nonexclusive license to make, modify, use and sell the prior invention as part of the product.

An "assignment of inventions" provision, meanwhile, should allocate ownership of intellectual property created while the employee works for the company. Typically, the employee should assign to the company all right, title, and interest in any inventions, original works of authorship, trade secrets, and other intellectual property developed while in the employ of the company. Any exceptions should be separately listed and clearly described.

Protect the employer's IP

Beyond protecting itself against accusations of misappropriation, an employer should lay a groundwork for protecting its own IP. To that end, onboarding documents should include a confidentiality provision or reference a standalone confidentiality agreement. This provision or agreement should clearly articulate (i) that the company maintains trade secret or other proprietary information, and (ii) how employees are expected to preserve the confidentiality of that information – both during and after employment.

Confidentiality provisions typically prohibit onboarding employees from disclosing confidential information to non-employees, accessing company systems using private devices, or removing confidential information from the premises. The employee should understand that he or she must accept these terms as a condition of employment. In most cases, the provision should alert the employee to the fact that the obligations will survive his or her employment at the company.

Confidentiality provisions are key to maintaining the trade secret status of proprietary information. This is because, under federal law and the law of most states, a trade secret owner must take "efforts reasonable under the circumstances" to maintain the secrecy of such information. As such, a good confidentiality provision will explain the employee's role in preserving that secrecy. If enforced, a good confidentiality provision will ensure that trade secrets are never improperly disclosed. Should improper disclosure nonetheless occur, the employer may point to the confidentiality provision as evidence that reasonable efforts were taken to protect the information.

Regularly review and update policies

Employers should periodically – at least annually – review and update onboarding documents to reflect changes in the law. For example, in 2016, Congress enacted the federal Defend Trade Secrets Act (DTSA). The DTSA provides whistleblower protection from prosecution to employees, independent contractors and consultants who disclose trade secrets if the disclosure was made to report or investigate an alleged violation of law. The DTSA further requires that employers include notice of such immunity in any agreement with an employee, contractor or consultant that governs the use of trade secret or confidential information. The DTSA is a reminder that companies should periodically consult with legal counsel to ensure that provisions remain compliant with newly-enacted laws or regulations.

Compliance for a digital, mobile age

Employers should also consider adopting policies to address risks associated with the contemporary, digital workplace – a workplace in which employees work from home, bring their own devices, and even represent the company on social media. Such policies include personal device and social media policies, each of which should be adapted to fit the employer's needs.

Adopt a personal device policy

Employers should establish a clear policy on the use of personal devices to access company data, including email. A strong policy will take into account the many risks of allowing employees to access company systems using private devices. Those risks include accidental disclosure of information to hackers exploiting lax security software on personal devices; purposeful disclosure of confidential information to friends and family; and the employer's general inability to monitor how the employee chooses to use the information, both during and after employment. Allowing employees to access sensitive information on personal devices may also violate NDAs with other companies – putting the company at legal risk – and may call into question whether the company has taken "reasonable steps" to maintain the secrecy of trade secret information. A court may find that a trade secret owner has forfeited the trade secret status of proprietary information if reasonable steps are not taken to preserve its secrecy.

Because of these risks, an employer may wish to adopt a blanket ban on the use of personal devices for company tasks. To the extent that personal devices are allowed, the company should place strict limits on what information may be stored on such devices. For example, employees may be permitted to access company email on a smartphone only if it is equipped with company-approved security software. In any event, the company policy should make clear that confidential or trade secret information should never be stored locally on a personal device or forwarded to private email accounts or servers.

Adopt a social media policy

Employers should also consider adopting a social media policy establishing clear guidelines for appropriate employee conduct on social media sites. Social media enables employees to freely share information of all kinds to a diverse audience. Improper use of social media, however, could endanger the company's reputation, alienate customers or clients, destroy the trade secret status of information through public disclosure, or even invite legal action against the company in the event that an employee discloses third party IP or commits an unlawful act, as by harassing a fellow employee.

At minimum, a social media policy should remind employees not to share sensitive company information online. A stronger policy may also specify that employees must brand their posts as personal and unassociated with the employer, or may even forbid employees from publicly sharing objectionable content, such as racial or ethnic slurs. To the extent that an employee is authorized to manage an official company social media site on behalf of the company – such as the company Twitter handle – a separate policy should impose more detailed guidelines governing the use of that account.

Implement and follow policies

Policies are only useful if they are actually implemented and enforced. Unworkable policies may look good on paper, but fall apart in practice. For example, a confidentiality provision may provide that any disclosure of confidential information to third parties must be approved in writing by the CEO. At most companies – especially larger companies that routinely share data with business partners subject to confidentiality agreements – this process will not be carried out in a consistent manner, if at all, because the CEO simply does not have time to focus on such matters. Instead, adopt a more reasonable, easier-to-implement policy that will not disrupt the company's operations. Rather than inflexibly requiring a single individual's sign-off, consider a review protocol that enables any one of several qualified executives to approve NDAs.

Companies should also avoid drafting policies that are confusing, nonspecific, or do not fit the company's products or business model. Skip the legalese and avoid off-the-shelf, "one size fits all" policies. If the company's own executives and employees do not understand the company's own policies, those policies will be ignored or inconsistently implemented. Consult with an attorney who is familiar with your company's needs and get your policies right from the start.

Begin with the end in mind

Onboarding is also an ideal time to look beyond a new employee's tenure at the company and lay a groundwork for his or her departure. Employers should build in rights up front – long before the exit interview – to ensure that the company has sufficient legal tools to protect its IP without need for litigation. By looking ahead, an employer can save a lot of hassle down the road.

Reserve personal device inspection rights

Employers should adopt a device inspection policy granting the company the right to examine a departing employee's personal devices to ensure that no sensitive company information remains on each device. The policy should make clear that all materials, communications or data created or stored on any device by the employee on behalf of the employer is the employer's property, regardless of who owns the device itself. The policy should further establish that the employer is entitled to monitor, review and erase all such content at any time.

Ensure continued control of social media accounts

Employers should further clarify that any social media accounts created on behalf of the company belong to the company, and that log-in information – including usernames and passwords – must be relinquished prior to the employee's departure. The employee should further agree to cooperate with the company – both during and after employment – to reestablish lost or suspended access to such accounts, if necessary.

With these practices, a company can help preserve its own trade secrets on the back end, and defend against accusations that an employee has misappropriated a former employer or third party's IP on the front end.
