SHEEHAN PHINNEY

PROTECT YOUR TRADE SECRETS:

Adopting a Proactive Employee Mobility Strategy

INTRODUCTION

Almost every company today is engaged in something of a multi-dimensional war. There is as intense a competition for talented employees, skilled workers and seasoned executives as at any time in our history. At the same time, there are challenges that animate and confuse the competition for talent.

CHALLENGES

Talent is exceptionally mobile – moving in unprecedented numbers and in an unprecedented manner. Employees do not observe old standards of company loyalty and longevity. The career employee seems to be largely a thing of the past; online tools for viewing and evaluating supposed greener pastures have come into widespread use and have become easier to use. Employees can post their resumes and credentials in dozens of sites. LinkedIn personal "networks" essentially function as job-sharing resources. And companies increasingly turn to recruiters to leverage the best employees out of one company and into another.

Additionally, employees have access to a broad universe of know-how, confidential and proprietary information and trade secrets, accessed and used with digital tools and systems that can capture, copy and send that information with breadth and speed. Employees are perhaps the biggest single threat to the competitive position of any company in any industry.

KNOW WHAT YOU HAVE: THE AUDIT

Every company needs an employee mobility strategy, one that accounts for the risks associated with employee mobility and requires skilled and experienced counsel. This "Employee Mobility and Trade Secret Protection Program" begins with an effort to understand what facets of the business might be important, confidential and secret, and to identify the manner and means by which that information can be protected. This is sometimes called an IP Audit or a Trade Secret Audit, either of which identifies information, formulae and processes that advance the company's competitive position and constitute protectable interests.

PROTECT WHAT YOU HAVE FROM MISUSE

Once the company understands what needs to be protected, it can secure the physical space effectively, and implement proper and proportionate internal security measures applicable to all employees, including system password protections, internet, email and text-messaging policies, and restricted access to trade secret information. Not every employee needs access to the company's pricing worksheets, for example.

Remote employees pose separate and different concerns, which should be addressed. Certain information should never be emailed, and certain information should be sent only with appropriate encryption. It is, perhaps, just as important as any other part of a policy to educate employees – making security and confidentiality a meaningful part of their daily lives, and creating an overall ethos within the company of care, caution and confidentiality.

NEXT

PROTECT WHAT YOU HAVE FROM MISUSE (CONT.)

The Program then determines the appropriate means to protect that information from use, misuse or misappropriation by existing and departing employees, usually through the creation, execution and enforcement of contractual agreements requiring the return of all company property at the end of employment, and containing so-called "post-employment restrictive covenants:" non-disclosure, non-solicitation, anti-piracy and non-compete provisions.

These sorts of agreements, though enforceable if narrowly tailored, are scrutinized by the courts, and need to be carefully constructed and measured against the company's legitimate interests in protecting information and employee, customer and other important business relationships.

PROTECT THE COMPANY AT THE GATEWAYS

The Employee Mobility Program should also game-plan for the issues posed by the onboarding of new employees and the exit of departing employees.

Hiring and Trade Secrets:
Most companies focus only on departing employees. But candidates and applicants for employment need, in many industries and disciplines, to be screened. Some questions and issues include these:

- Has the company made it clear from the outset that it honors the reasonable and valid post-employment obligations?
- Has the company made clear from the outset that the employee should neither bring nor use any confidential information from a prior employer?
- Do they currently work for a competitor?
- Do they have post-employment agreements that restrict or disable their ability to work for you?
- Are those agreements valid and enforceable against the employee if she joins your company in the anticipated role(s)?
- Does that agreement include a provision requiring "return of company property"? If the applicant has already departed, has she carefully honored this obligation?
- Do they possess knowledge that their former employer might consider confidential and at risk in the new role with your company?

Resolution of these and other questions in advance of making an offer can resolve a potentially deep thicket of discord and, maybe, litigation with the former employer.

Departure:
The departing employee poses more and different risks. The departure of an employee, particularly to a competitor, opens a window to the loss of important confidential information and trade secrets, as well as valuable goodwill residing in that departing employee. Once the company knows an employee is leaving, it should take certain steps to prevent continued access to information and assets

NEXT

and to remind the person of their ongoing obligations. These steps include what should be a familiar checklist:

- Shutting off access to email and other internal and external communication systems;
- Placing automatic notifications on email and cell phones to direct business callers to the person now responsible for the duties once carried out by the departing employee;
- Removing movement privileges around the facility;
- Sequestering of company-owned and issued laptops, phones and other devices so that evidence of activities in the immediate term can, if necessary, be reviewed and preserved;
- Gathering of all other company property; and
- Conducting an exit interview that includes an explicit discussion of post-employment obligations and a description of the categories of information that the company considers confidential, proprietary and trade secrets.

Every company hopes to retain employees who materially help carry out the company's mission. But planning for departure from Day One – and putting into place an Employee Mobility and Trade Secret Protection Policy and Program – is prudent and necessary in today's workplace.

For legal guidance with your Employee Mobility strategy, please email pvoegelin@sheehan.com

Boston Office
28 State Street, 22nd Floor
Boston, MA 02109
Phone: 617.897.5600
Fax: 617.439.9363

Manchester Office
1000 Elm Street, 17th Floor
Manchester, NH 03101
Phone: 603.668.0300
Fax: 603.627.8121

Concord Office
Two Eagle Square, 3rd Floor
Concord, NH 03301
Phone: 603.223.2020
Fax: 603.224.8899

Upper Valley Office
15 Railroad Row, 2nd Floor
White River Jct, VT 05001
Phone: 603.643.9070

Portsmouth Office
75 Portsmouth Boulevard, Suite 110
Portsmouth, NH 03801
Phone: 603.431.1222

To learn more, visit sheehan.com