PRACTICAL
PERSPECTIVES

Sten-Erik Hoidal
612.492.7334
shoidal@fredlaw.com

Timothy O'Shea
612.492.7373
toshea@fredlaw.com

BEST PRACTICES FOR DATA PROTECTION

Steps to Protect Confidential and Trade Secret Information

(1) Conduct a Data Protection Audit

- Determine what information is confidential or trade secret, who has access to such information, and where it is stored.
- Periodically review this information to make sure only confidential and trade secret information is being treated as such, that only those employees with a need to know have access to the information, and that the information is secure.

(2) Deploy Security Measures And Policies

- Use physical and electronic security measures such as access controls for the building and areas within the building, locked doors and cabinets, password protected files or encryption, ID badges for employees, restricting the location/time/ and access to such information, labeling documents as confidential and trade secret.
- Train employees on the importance of confidentiality and define what that information entails and address how such information should be handled and protected in employee handbooks.
- Limit access of confidential information and trade secrets to a discrete group of individuals who need the information to perform their jobs.

(3) Use Appropriate Contractual Protections

- Employers should include confidentiality clauses in employment agreements for those employees who will have access to confidential and trade secret information. The confidentiality clause should sufficiently define the company's confidential and trade secret information and make clear that access to and use of such information shall be solely for the benefit of the company and not the worker.
- A non-disclosure agreement with employees or any third parties given access to confidential data is critical for protecting confidential information and trade secrets.
- A non-compete agreement provides enhanced protection to employers by creating barriers to competitive activity for departing employees and effectively prohibiting them from using the employer's trade secrets and confidential information for a competitor.
- A non-solicitation agreement indirectly protects trade secrets by limiting a former employee's freedom to "raid" company resources, such as employees and clients.

(4) Implement A Clear, Enforceable Policy Relating To Authorized Use Of Company Property

- Implement an electronic policy that alerts employees that computers are company property and remind them that the company reserves the right to monitor employees' emails, internet, and computer use (i.e., that the employee has no expectation of privacy).

(5) Implement Procedures For Departing Employees

- Conduct exit interview, eliminate access to computer systems, require return of all company documents and information, request acknowledgment that employee has complied.

Fredrikson & BYRON, P.A.

Steps to Take to Avoid Potential Claims From Former Employers For Theft of Trade Secrets

(1) Determine If Applicant Is Subject To Any Post Employment Restrictions

- Ask applicant to identify any agreements with their current or former employer that contain confidentiality or non-compete provisions.
- Ask applicant to provide all documents that might contain employment restrictions such as non-disclosure agreements, confidentiality agreements, non-compete agreements, non-solicitation agreements, invention assignment agreements, and general employment agreements.

(2) Assess The Enforceability of The Restrictions In Applicants' Employment Agreements

- Enforcement of restrictions depends on a number of factors such as (a) whether the applicant will actually be engaging in the prohibited activity in the new position, (b) what activities are restricted, (c) whether the former employer is entitled to restrict that activity, and (d) the law in the relevant jurisdiction.

(3) Tailor The Offer Letter And Remind Prospective Employees Of Their Obligations

- An offer letter should remind prospective employees that they need to abide by any enforceable restrictions with their former employer and that failure to do so is a terminable offense.
- An offer letter should remind prospective employees that they should not take copies of their former employer's confidential and trade secret information and should return all of their former employer's property (such as laptops, PDAs, smartphones, thumb drives, and hard copies of work-related documents).
- Have the employee sign an acknowledgment that they do not have and will not disclose any of their former employer's confidential and trade secret information.

(4) Review Job Assignment For Potential Employee If Risk Of Litigation Is High

- Before hiring an applicant, assess the risk that a former employer will file suit against the company or its new employee.
- Consider modifying the position so that the new employee is performing tasks that are different than what the applicant did for the former employer.

(5) Coach Employees Against Use Of Former Employer's Confidential And Trade Secret Information

- Consider drafting a policy explaining that the company expects its employees not to use or disclose former employer's confidential and trade secret information.
- Coach employees to dissuade other employees from using former employer's confidential and trade secret information and to report any such use.