

TRADE SECRET PROTECTION GUIDELINES

I. Trade Secrets: An Alternative to Patent and Copyright Protection

In the process of securing patent protection, a company may be faced with the dilemma of having to disclose a company's trade secrets or risk jeopardizing the validity or enforceability of any patent that ultimately may issue. In such a case, a company needs to weigh the value the trade secret that will be lost if disclosed in the patent process against the value of the patent protection to be gained. In some cases, the trade secret may be more valuable to the company than the patent likely to issue. Or, patent protection just may not be available. Likewise, with copyright protection, although the author can mask the work (ie, source code) to be submitted to the Copyright Office, so as to protect against the disclosure of a company's trade secrets, copyrights, like patents, are wasting assets, in that their respective lives are of limited duration. Trade secrets are of infinite duration, at least theoretically, as long as secrecy is maintained. These Guidelines are directed to companies who have made the decision to identify, protect, and maintain trade secrets as valuable intellectual property assets of the company, and are in need of guidance as to how to implement a winning trade secret protection program.

A. Differentiating Among Trade Secrets and Confidential/Proprietary Information

1. Trade Secrets

Examples of trade secrets include engineering information; methods, processes, and know-how; tolerances and formulas; business and financial information; computer programs (**particularly source code**) and related information; pending, unpublished patent applications; business plans; budgets; methods of calculating costs and pricing; customer and supplier lists; internal marketing data; specifics concerning customers and suppliers; products and services in research and/or development; collections of data; and other information relating to a company's business.

To be a trade secret, the subject information must not be generally known to the public or to persons outside of the company who are knowledgeable about the general subject matter of the information. To be a trade secret, information must be sufficiently secret to confer an actual or potential economic or business advantage or benefit upon one who possesses the information.

2. Confidential Information

All trade secrets are confidential information but business information that may not rise to the level of a trade secret may also be deemed confidential within the company. This includes any documents or physical objects marked as confidential, categories of documents and objects designated as confidential, physical areas designated as confidential, procedures, processes, and methods, computer programs, and any other information, objects, locations, and the like that the company wishes to treat as confidential by any means.

3. Proprietary Information

All trade secrets and confidential information are also company proprietary information, but proprietary information may also include information that is not secret in any way, such as copyrighted information and the subject matter of patents. In fact, a company may view as proprietary virtually everything it does or creates, even if some of it is not protectable as a form of intellectual property. For example, a company's philosophy of customer management may be considered proprietary, even though the philosophy itself may not be protectable in any way.

Unfortunately, many business people and documents use the terms "trade secret," "confidential," and "proprietary" interchangeably or inconsistently. Although trade secrets and confidential information may have the same meaning in some contexts, they may not mean the same in other contexts, and the term "proprietary information" may often be used generically. In short, trade secrets and confidential information are a subset of the potentially much larger class of proprietary information. Moreover, if these terms are all used in an agreement, courts may infer that each term has a separate meaning even if the parties' intent was that they have interchangeable meanings, or worse, that the parties did not know what they meant by their loose use of these terms.

B. Documentation of Trade Secrets

Trade secrets should be documented whenever possible, in paper or electronic form. Though the company may not wish to document some trade secrets for fear that some important secrets may be omitted from the documentation process, the better approach, on balance, is to spend time identifying trade secrets and to document their secret status and the value that their secret status confers on the company. In *Lynchval Systems, Inc. v. Chicago Consulting Actuaries, Inc.*, 49 U.S.P.Q. 2d 1606 (N.D. Ill. 1998), the plaintiff lost on defendants' motion for summary judgment because it failed to meet its burden of persuasion that it actually viewed and treated the alleged trade secrets in suit as company secrets before filing suit. In litigation, courts may require the trade secret owner to identify its alleged secrets before discovery relating to the defendant's alleged misappropriation can begin. Thus, the company needs to be prepared to identify its trade secrets and to show that it has in fact viewed and treated them as such.

C. Notice of Confidentiality and Marking of Documents

All trade secrets should be accompanied by a notice of confidentiality or be marked or designated as confidential information. An example of such a notice, to be stamped or otherwise applied to the first or main title page of all trade secret documents in either paper or electronic form, is as follows:

CONFIDENTIAL

This document contains trade secrets or otherwise confidential information owned by the Company. Access to and use of this information is strictly limited and controlled by the Company. This document may not be copied, distributed, or otherwise disclosed outside of the Company's facilities except under appropriate precautions to maintain the confidentiality hereof, and may not be used in any way not expressly authorized by the Company.

The words "Confidential Information of the Company", or similar words, should be stamped or otherwise applied to all other pages of such documents.

When trade secrets cannot be marked as such, they should be accompanied by a notice of confidentiality or otherwise designated as confidential by a method appropriate under the circumstances. For example, physical facilities containing or constituting trade secrets may be designated as confidential by posting appropriate signs or placing appropriate labels on hardware or computer monitors. As another example, electronic media, e-mails, or electronic files containing trade secrets should bear or be accompanied by an appropriate notice of confidentiality. The following is a sample notice of confidentiality that can be modified as appropriate under the circumstances.

CONFIDENTIAL

[This equipment contains trade secrets or otherwise confidential information owned by the Company] or [Trade Secrets or otherwise confidential information owned by the Company are used in this area]. Access to and use of this [equipment/area/information] is strictly limited and controlled by the Company. Such trade secrets may not be used or disclosed outside of the Company's facilities except under appropriate precautions to maintain the confidentiality hereof, and may not be used in any way not expressly authorized by the Company.

Questions regarding whether or how to mark or otherwise designate documents or other information as trade secrets should be directed to intellectual property counsel.

D. Non-written Disclosures

Trade secrets may be disclosed orally during meetings between parties. Ideally, such oral disclosures are made under a confidential disclosure or "nondisclosure" agreement, and should always reveal only as much trade secret information as is required under the circumstances. However, the relative bargaining power of the parties can substantially reduce or even eliminate the value of such an agreement. The more sophisticated a company is, the more likely that it will require the disclosing party to accept its own nondisclosure agreement, which may so favor the company that the disclosing party is virtually unprotected. Other companies with sufficient bargaining power may refuse to sign nondisclosure agreements.

This can be a problem when trade secrets are or may be disclosed in non-written form during discussions between parties. Such disclosures could be oral in nature, or they could be made through the exchange of sample devices or products. In such situations, it is important that the trade secret owner must not disclose secrets at all, or should do so only under an agreement providing that oral or other non-written disclosures shall be treated as secret. The agreement may require that oral or other non-written disclosures must be memorialized before disclosure. However, the agreement should also provide that if oral or non-written trade secrets are not memorialized before they are disclosed, they can be described and reduced to writing after disclosure. The agreement should provide that oral and non-written trade secrets must be identified, reduced to writing, and designated as such within a certain number of days after disclosure, and that the receiving party's obligation to preserve such secrets is contingent upon the disclosing party identifying the secrets and reducing them to writing.

E. Due Diligence

The company, in the form of its directors, officers, supervisors, and employees, should regularly assess all company information within their purview to determine what information should be maintained as trade secrets, and to take appropriate steps to maintain the secrecy of such information. It is advisable to err on the side of maintaining the secrecy of company information.

II. Preservation of Trade Secrets and Other Confidential Information

A. Protection of Trade Secrets in Relations with Employees

1. Employee Obligations

As a condition of initial or continued employment, all employees should be required to sign a non-confidential employment agreement setting forth their obligations with respect to the company's trade secrets and other matters. The permissible scope and enforceability of such agreements varies from state to state. The company should enforce such agreements to the fullest extent of the applicable law. The company's failure to do so could affect its right or ability to enforce the same or another agreement in other instances.

2. Procedures for New Employees

All new employees should be required to sign the company's standard employment agreement, which should evolve with the times. A designee of the Human Services Department should meet with each new employee within five (5) working days after the commencement of the employee's employment. Such person should:

- a. Explain the company's trade secret policy and provide the employee with a copy of the policy.
- b. Ask the employee if he/she retained any information, documents, or physical objects (including computer programs, manuals, or design documentation) from his/her prior employer(s) after leaving such employment, and whether he/she signed a confidentiality agreement with prior employers.
- c. Ask the employee the nature and subject matter areas of the work performed for prior employers (however, instruct the employee not to reveal any trade secrets or confidential information of any prior employer when answering this question).
- d. Instruct the employee that he/she may not use or bring into the company's facilities or computers (by any means) any information, documents, or physical objects learned or obtained from any prior employer or considered to be proprietary by any other person.
- e. Inform the employee that under certain circumstances the company may need to contact the employee's former employer(s) regarding the scope of the employee's obligations to his/her former employer(s) or regarding the employee's answers or comments to items a-d above.
- f. Ask the employee if he/she understands items a-e above.
- g. Prepare a report, simultaneously with the meeting, documenting the employee's answers and comments regarding items a-f above.

If the employee answers affirmatively to item b above, will be performing substantially the same nature of work or will be working in substantially the same subject matter areas for the company as for any prior employer, or disagrees with any of items a-e above, the person conducting the interview should seek legal advice immediately so that appropriate action can be taken. The company should also consider contacting an employee's former employer(s) when, in the judgment of the appropriate officer of the company and legal counsel, such contact is likely to reduce the risk of a dispute between the company and any employee's former employer(s). If the employee has signed a confidentiality agreement with a former employer, the company should review such agreement unless the terms of the agreement itself are confidential.

3. Procedures for Departing Employee

An appropriate designee of the Human Services Department should meet with each departing employee no more than five (5) working days prior the employee's last day of employment, unless an employee departs the company abruptly or without notice. In such situations, the HSD representative should try to speak to the employee before or even after he/she departs. Such person should:

- a. Inform the employee that various obligations of his/her employment survive the termination of employment, and that the employee must continue to comply with such obligations, such as trade secret obligations, set forth in the employment agreement.

b. Ask the employee if he/she plans to retain any information, documents, or physical objects (including files, computer programs, manuals, or design documentation) after leaving the company's employment. If so, ask the employee to identify all such information, documents, and physical objects, and instruct the employee not to take any such items that the company views as secret or otherwise proprietary.

c. Ask the employee the nature and subject matter areas of the work expected to be performed for his/her next employer (however, instruct the employee not to reveal any trade secrets or confidential information of his/her next employer when answering this question).

d. Instruct the employee that he/she may not use or bring into any future employer's facilities or computers (by any means) any information, documents, or physical objects learned or obtained from the company or considered to be proprietary by any other person to which the company has any legal obligations.

e. Inform the employee that the company may take legal action against the employee and/or his/her future employers, without prior notice, for using or bringing into any future employer's facilities or computers (by any means) any specific information, documents, or physical objects learned or obtained from the company or considered to be proprietary by any other person to which the company has any legal obligations.

f. Inform the employee that under certain circumstances the company may need to advise the employee's next employer of the employee's obligations under his or her employment agreement, and that he/she can show such employment agreement to the new employer.

g. Ask the employee if he/she understands items a-f above.

h. Prepare a report, simultaneously with the meeting, documenting the employee's answers and comments regarding items a-g above.

If the employee answers affirmatively to item b above, will be performing substantially the same nature of work or will be working in substantially the same subject matter areas for his/her next employer, or disagrees with any of items a-f above, the person conducting the interview should seek legal advice immediately so that appropriate action can be taken. The company should contact an employee's next employer when, in the judgment of the appropriate officer of the company and legal counsel, such contact is likely to reduce the risk of a dispute between the company and the employee's next employer, or when such contact appears to be necessary to reduce the risk that the employee and/or his/her next employer will learn or use any company trade secrets. When an employee is terminated or laid off, steps should be taken before informing the employee of such termination or layoff to secure trade secrets and other proprietary information to which the employee has access.

B. Protection of Trade Secrets in Relations with Non-Employees

1. Agreements with Independent Contractors

As a condition of initial or continued engagement, all independent contractors should be required to sign an agreement setting forth the contractor's obligations with respect to the company's trade secrets and other matters. The company should have the right to change such agreements from time to time. As a condition for continued engagement, and to reduce uncertainty regarding the contractor's obligations at any particular time, the company should require contractors to execute

the company's current contractor agreement. The permissible scope and enforceability of such agreements varies from state to state.

2. Agreements with Other Companies

Trade secrets must not be disclosed to persons or entities other than company employees or independent contractors who have executed appropriate employment or other contracts, unless such persons or entities execute appropriate confidential disclosure agreements or other agreements containing sufficient confidentiality obligations to protect the company. Such agreements should be prepared and/or approved by legal counsel. The obligations of recipients of trade secrets under such agreements should be perpetual unless the trade secrets become publicly known through no act or omission of the recipients, or other reasons exist for specifying a shorter trade secret term.

C. Internal Security Measures

All of the company's officers, managers, directors, and supervisors should assure that the following security measures are instituted and followed, as appropriate, with respect to all trade secrets. Questions regarding which security measures should be used in any particular circumstances, how to follow and enforce such security measures, and how to handle breaches of such security measures, should be directed to legal counsel.

1. Materials containing trade secrets must be marked, stored, and handled with sufficient care to maintain their confidentiality. Trade secret information not reduced to documented form must be maintained with sufficient care to maintain its confidentiality.
2. Documents, physical objects, and undocumented information (such as processes) containing or constituting trade secrets must not be left in plain view and must not be accessible to any persons (particularly non-employees, such as visitors) who are not authorized to have access thereto and who have not signed an agreement with the company containing appropriate confidentiality obligations to the company.
3. Documents containing trade secrets must be maintained in secure locations, under lock and key when possible, when not in use and after business or work hours.
4. When appropriate, such documents should also be maintained in a finite number of copies and authorized persons accessing such copies should be required to sign them out, sign them in, not make any copies, and maintain possession of such copies only for a finite period of time.
5. Trade secret information stored in computers, in magnetic media, or on other devices should be password or copy protected and/or encrypted, and must not be accessible to unauthorized persons or through the Internet, email, or any other form of electronic communication.
6. Employees must be reminded periodically of their confidentiality obligations, and that maintaining such obligations is a condition of their employment. Such reminders should be made no less than twice annually.
7. Unnecessary copies, whether electronic or paper, containing trade secrets should be destroyed.
8. Visitors to the company's facilities should be required to sign in and to sign out, should be escorted by a company employee at all times, and must wear "Visitor" badges at all times. The

company employees with authorized access to secret areas may not take visitors to such areas unless such visitors have executed an appropriate confidentiality agreement.

9. Trade secrets must not be disclosed to any person owing no obligations of confidentiality to the company.

10. Employees may not download or otherwise transfer or transmit trade secrets to their home computers, remove materials containing trade secrets from the company premises, or disclose trade secrets to persons under no obligation of confidentiality to the company except with prior, express, written permission of an officer or designated employee of the company with authority over such trade secrets.

11. The company should have written trade secret policies and procedures, and employees should be educated and periodically informed of such policies and procedures.

12. The company should appoint a trade secret officer or committee to prepare, disseminate, and enforce the company's trade secret policies and procedures.

D. Speeches and Technical Papers

The presentation of any speeches or technical papers containing any trade secrets by any employees to any person(s) not under an obligation of confidentiality to the company should be authorized in advance in writing by an officer the company. This pre-clearance is required to:

1. prevent an inadvertent disclosure of the company's trade secrets;
2. provide the opportunity for a review of the technical accuracy of papers or speeches; and
3. provide the time and opportunity to prepare and file patent applications, if appropriate, before the information set forth in such speeches or papers is disclosed to the public.

If any such speeches or papers relate to the subject matter of any joint venture between the company and any other entity, or include any information that may be considered proprietary by any other entity, the company officer or designated employee with authority over such trade secrets should seek legal advice regarding the disclosure of such information.

E. Limited Access to Trade Secrets

Only employees who need to know a trade secret for purposes of carrying out their employment duties may have access to such trade secret. The company should ensure that trade secrets are accessible only to employees with such need to know them, and only to the extent necessary for such employees to carry out their duties. Access should be appropriately limited to the particular materials containing the information the employee needs to know.

F. Demonstrations

Demonstrations of company products or processes may be made at trade shows, customer meetings, or in other situations. However, trade secret aspects of such products or processes should not be revealed in demonstrations unless the person(s) receiving the demonstration have signed a confidential disclosure agreement.

III. Conclusion

These Guidelines are intended to be a general overview of trade secret principles. Particular

trade secret situations are very fact dependent and could require treatment different from or more complex than the principles set forth in these Guidelines. Thus, these Guidelines should not be regarded as legal advice>