

TRADE SECRET PROTECTION PLAN CHECKLIST

To determine how to establish and maintain a Trade Secret Protection Plan, it is important to first understand what a trade secret is.

California Civil Code Section § 3426.1(d) defines a trade secret as:

Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

- (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
- (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

By definition, a trade secret may be almost anything which has economic value and advantage over a competitor. However, a trade secret owner must take (or have taken) reasonable steps to safeguard the secrecy or confidentiality of the information (or other thing) that the owner wants to claim as a trade secret. If a trade secret is not kept secret, the legal protections afforded to them will be lost.

1. Trade Secret Protection Plan: Identify Trade Secrets.

(A) Using the definition above, key people in the company should determine what confidential information, processes or other things that give the company an advantage over its competitors constitute trade secrets.

Trade secrets may be:

- Computer Programs (including programmer's notes)
- Business Know-How (what works and what doesn't)
- Specifications, Bill of Materials, Recipes, and the like
- Processes (including flow charts)
- Formulas (including algorithms)
- Distribution Sources
- Business Methodologies
- Customer Information (lists and preferences)
- Financial Information
- Vendor/Supplier Lists (not readily available from public sources)
- Business and Marketing Plans

- Product/Service Pricing
- Personnel Information
- Machinery (developed, utilized or unique to the company)

(B) The following questions may help identify a company's Trade Secrets:

- Is the information/process secret?
- Is the information/process valuable?
- Is the information/process known in the industry?
- Is the information/process obvious to others?

2. **Conduct an Initial Trade Secret Audit.** To ensure trade secret protection, routinely conduct an audit to determine 1) what measures are in place to secure trade secrets, 2) whether these measures are effective, and 3) what additional measures, if any, need to be put in place.

The following questions can help organize an audit:

- Are there procedures in place to identify trade secrets?
- Are there any measures currently in place to safeguard trade secrets?
- What are they?
- Where are the trade secrets located?
- Who has access to them?
- Are written policies concerning safeguarding trade secrets in place?
- Who signs nondisclosure agreements? Why?
- What can be done further to safeguard trade secrets?

3. **Develop a Trade Secret Protection Plan.** A trade secret protection plan should be in writing and reflect reasonable efforts under the circumstances to safeguard your organization's trade secrets.

Efforts to safeguard trade secret status may include the following measures discussed in more detail in paragraphs 4-15 of this checklist:

- Segregate Trade Secrets from Non-Trade Secrets
- Label Documents, Items and Software Containing Trade Secrets
- Execute Nondisclosure Agreements
- Use Employee Manuals to stress trade secret protection
- Conduct Employee/Contractor Orientation and Education
- Use Notice Measures
- Use Physical Security Barriers
- Take Additional Steps to Keep Confidential Documents Secret

- Prevent Inadvertent Dissemination of Trade Secrets to Others
- Conduct Exit Interviews with Departing Personnel
- Limit Access to Visitors
- Conduct Routine Trade Secret Audits

4. **Segregate Trade Secrets.**

Trade secrets should be segregated from non-trade secrets to differentiate between what the company regards as a trade secret and what it does not. By keeping the trade secret items/information separate from the non-trade secret items/information, the company's claim of trade secret status has a much better chance of being preserved.

5. **Label Documents, Items and Software Containing Trade Secrets.**

Label trade secret materials using the following or similar legends:

- "TRADE SECRET," "SECRET," "CONFIDENTIAL," or "CONFIDENTIAL INFORMATION."
- "TRADE SECRET. This document contains confidential and proprietary information of [company name]. Do not copy or circulate."
- "CONFIDENTIAL INFORMATION. [company name] (Unpublished) All rights reserved."
- "PROPRIETARY INFORMATION. [company name] (Unpublished) All rights reserved."
- Create headers or footers on documents and software as follows:

"This document contains confidential and proprietary information of [company name] and is protected by copyright, trade secret and other State and Federal laws. Its receipt or possession does not convey any rights to reproduce, disclose its contents, or to manufacture, use or sell anything it may describe. Reproduction, disclosure, or use without specific written authorization of [company name] is strictly forbidden."

6. **Nondisclosure Agreements.**

- All Employees, independent contractors, consultants, vendors, suppliers, licensees, and others that may, for any reason, access trade secrets should sign nondisclosure agreements.
- At a minimum, nondisclosure agreements should be signed by employees, consultants, contractors, vendors, and others who have access to (or will have access to) trade secret information and documents.
- Employees, consultants, contractors, vendors, etc., should sign nondisclosure agreements **before** the trade secret information/items are seen, discussed or revealed.
- Employees, consultants, etc. should read and sign the nondisclosure agreement on or before the first day of work.

7. **Employee Manual**. If an Employee Manual exists, include:
- A section discussing the company's Trade Secret Protection Plan and employees' obligation under their Nondisclosure Agreements.
 - Have employees sign a memorandum on the first day of employment that they have read the Employee Manual and understand the company's Trade Secret Protection Plan.
 - Place the memorandum in the employee's personnel file.
8. **Employee/Contractor Orientation and Education**. Employees/Contractors should understand the elements and ramifications of their company's Trade Secret Protection Plan from the first day of work.
- Mandate that new employees/contractors not disclose the trade secrets of others (e.g., former employers).
 - Explain that company trade secrets and confidential information cannot be disclosed outside the company.
 - Make clear that disclosure of trade secrets and proprietary information are grounds for termination.
 - Have all employees/contractors sign Nondisclosure Agreements.
 - Remind employees at their reviews of your Trade Secret Protection Plan and their duty under the Nondisclosure Agreement they signed.
 - Discuss the company's Trade Secret Protection Plan at employee meetings.
 - Educate employees about industrial espionage and help employees identify and report those who might attempt trade secret theft.
9. **Notice Measures**. Notice measures should be promulgated. Samples include:
- Routinely remind all persons of their obligations under the Nondisclosure Agreements
 - Routinely remind all employees of the company's Trade Secret Protection Plan as discussed in the Employee Manual.
 - Key personnel should demonstrate by action the procedures set forth in the company's Trade Secret Protection Plan.
 - Distribute newsletter and/or memoranda that discuss the company's Trade Secret Protection Plan.
 - Place relevant posters in the work place, such as in the employee lounge, kitchen or rest area.
10. **Physical Security Barriers**. All trade secrets should be kept from unauthorized persons as follows:
- Block access to persons who do not need to know.

- Keep trade secrets in a locked room with “Private,” “Authorized Personnel Only” or “No Admittance” posted on the door.
- Keep trade secrets under lock and key in appropriate file cabinets.
- Use a log to list who has access to the confidential information.
- Use access codes to enter buildings.
- Encode or encrypt trade secret information.
- Lock laptops and storage materials in safes or filing cabinets.
- Computers should have appropriate access codes, passwords and security software.
- Change access codes or passwords after an employee/contractor has left the company.
- Create an environment of confidentiality.
- Implement a clean desk policy.
- Maintain all confidential information out of sight.

11. **Additional Steps to Keep Confidential Documents Secret.**

- Serialize and log trade secret documentation and materials.
- Safeguard faxed and photocopied documents from getting into the wrong hands.
- Trade secret documentation should not be faxed. If a trade secret document must be faxed, use a secured line and mark the materials with the appropriate trade secret legends.
- Trade secret documentation should not be e-mailed. If a trade secret document must be e-mailed, use proper encryption technology and/or security keys. Additionally, mark the materials with the appropriate trade secret legends.
- If trade secret documents or software are duplicated by any means, a log should be kept to show who copied the document or software, and where the duplication is going.
- Shred all confidential documents that are duplications, are not needed or are no longer in use.

12. **Prevent Dissemination of Trade Secrets or Confidential Information to Others.**

- Presentations, public speeches, web site information, press releases and all information that is to be disseminated to others should be scrutinized by the appropriate manager so no trade secret is leaked or unwittingly disclosed.
- Employees, contractors, consultants, and others should be required to obtain permission if they desire to disclose or use information/items that may be confidential, proprietary or trade secrets.

13. **Conduct Exit Interview with Departing Personnel.** At employee/contractor exit interview:

- Review the terms of the nondisclosure agreement with departing personnel and ask him/her to contact the company if they have questions with respect to the nondisclosure agreement.
- Remind employee/contractor of duty not to use or divulge company's trade secrets
- Require that the employee sign a termination certificate, if possible, acknowledging employee's/contractor's understanding and duty not to disclose trade secrets or confidential information.
- Obtain trade secret materials and documents in the employee's possession or control, including, without limitation, hard copies, diskettes (and other storage materials), home computer files, home office files, laptops, cell phones, etc.
- Require that keys and access cards be returned.

14. **Visitors.** Do not allow visitors (including repair or service persons) to wander freely. Incorporate the following procedures:

- Use a visitor's log book.
- Escort visitors.
- All trade secret/confidential information should be maintained out of sight at all times.
- Use nondisclosure agreements.
- Prohibit photography.
- Drape machinery that need not be seen.
- Maintain files out of sight.
- Restrict trade secret areas from access.

15. **Conduct Routine Trade Secret Audits.**

- On a routine basis, establish a program to identify new trade secrets.
- Review the existing Trade Secret Protection Plan and update the plan as necessary.