Trade Secret Protection and Management System

For any inquiries or feedback concerning this document, please contact us at:
creativeIP@iii.org.tw

For the Chinese version, please refer to:

https://stli.iii.org.tw/publish-detail.aspx?no=58&d=7212

Version 2023

Published 2025

Table of Contents

Introduction

The Trade Secret Protection and Management System is a management model for trade secrets, which may be introduced at the discretion of each organization. The purpose of this document is to guide organizations to establish a systematic trade secret management system based on relevant laws and regulations and operational objectives, thereby reducing the risk of trade secret leakage and enhancing organizational competitive advantage.

This document establishes trade secret management planning, implementation (including trade secret determination, trade secret usage control, employee management, network and equipment management, external activity management, and trade secret dispute handling), as well as monitoring and improvement, enabling organizations to establish a systematic trade secret

protection management system through the use of the "PDCA management cycle" (Plan-Do-Check-Act).

This document is used as the basis for internal audit or external certifications of the organization's trade secret management system, and help the organization to:

(a) ensure that its system is consistent with the organization's prescribed trade secret management policies and objectives;

(b) establish a trade secret management system that conforms to the requirements of this document;

(c) implement, maintain, and continuously improve the trade secret management system.

1. Scope

The requirements of this document are designed to be applicable to all organizations, regardless of type, scale, or the products or services they provide. The organizations can determine its management processes and methods based on the requirements of this document, taking into account factors such as their scale, attributes, and product or service characteristics.

2. Terms and Definitions

The relevant terms used in this document are defined as follows:

2.1 Trade Secret (TS)

It refers to that which complies with the Trade Secret Act of the country in which the organization is based.

2.2 Organization

It refers to a group formed to achieve specific objectives. A unit or project team within an agency or institution can also be considered an organization as defined in this document.

2.3 Documentation

It refers to establishing and presenting the processes and requirements of trade secret management. The presentation can be made available in any form, not limited to paper, including electronic media, audiovisual materials or software.

2.3 Controlled Area

It refers to spaces within the organization that contain trade secrets and are subject to control, such as file rooms, laboratories, offices, computer rooms, floors, etc.

2.4 Recording Media

It refers to media that store information in digital or analog formats, such as hard drives, flash drives, memory cards, optical discs, magnetic tapes, etc.

2.5 Information Equipment

It refers to equipment that can process information, signals, images, sounds, and exchange information with other information devices, such as computers, servers, smartphones, etc.

2.6 External Entities

It refers to external parties that may come into contact with the organization's trade secrets, such as customers, affiliated enterprises, suppliers, contractors, commissioned R&D entities, collaborative R&D partners, law firms, intellectual property service providers, etc.

3. Overall Planning

3.1 Roles and Attitudes of Top Management

3.1.1 Top management shall clearly define trade secret management policies and objectives, and ensure the establishment of a trade secret management system.

3.1.2 The establishment of the aforementioned policies, objectives, and management systems shall consider:

(a) organization-related internal and external issues, and relevant interested parties;

(b) appropriateness for the organization's scale, activities, and the nature of its products or services;

(c) compliance with relevant laws and other requirements that the organization must follow.

Note 1: Internal issues can include organizational values, culture, knowledge, competence, development strategies, and performance-related issues.

Note 2: External issues can include the impact of legal, technological, competitive, market, cultural, social and economic environmental issues from both domestic and international.

Note 3: Interested parties can include shareholders, internal personnel of the organization, external providers such as outsource or procurement organizations, customers, competitors, government agencies, etc.

3.2 Responsibilities and Communication

3.2.1 Top management shall ensure that the authorities for trade secret management are clearly assigned and made known to the members of the organization.

3.2.2 Top management shall personally or designate personnel/team responsible for the following:

(a) ensuring that the entire organization is aware of the policies and objectives of trade secret management;

(b) ensuring that the processes required by the trade secret management system are established, implemented, and maintained;

(c) ensuring that the aforesaid processes are delivering their intended results.

3.3 Management Review

Top management shall review the trade secret management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. Management reviews shall be planned and implemented with consideration of:

(a) the status of the actions from previous management reviews;

(b) the planning of and changes to the management system, including policy and objective setting, developing strategies, and changes in internal and external issues, etc. ;

(c) the implementation results of the management system, including the extent to which management objectives have been met, the status of the organization's trade secret management, trade secret audit results, and the implementation of major corrective actions.

3.4 System Planning

3.4.1 The organization shall establish, implement, and maintain the necessary trade secret management processes according to its scale and type to satisfy the requirements of this document.

3.4.2 The organization shall maintain documented information to the extent necessary to support the operation of the trade secret management processes, and shall retain documented information to the extent necessary to demonstrate that the processes are carried out as planned.

3.5 Resources

The organization shall determine and provide the resources needed for implementation, maintenance and continual improvement of effectiveness of the trade secret management system.

Note: Resources may include human resources, hardware and software facilities, network and software services, funding, etc.

3.6 Documented Information

3.6.1 The organization's trade secret management system shall include:

(a) a general description of the trade secret management system, including management targets, scope, accountabilities and job delegation, and the documented information established by the organization for the management system, etc.

(b) disciplinary rules for violations of the organization's trade secret management regulations;

(c) trade secret dispute handling mechanism;

(d) documented information determined by the organization.

3.6.2 The creation and updating of documented information shall meet the following requirements:

(a) reviewed and approved prior to announcement issuance and external disclosure;

(b) reissued through announcement when revised or updated.

4. Determination of Trade Secrets

4.1 Distinguishing Trade Secrets

The organization shall evaluate and distinguish trade secrets that are produced or acquired, and shall record the time and source of such production or acquisition.

Note: Sources of trade secrets can include duty-related outputs, outputs produced by third parties commissioned with funding, jointly developed outputs, trade secrets obtained through assignment or licensing, and other trade secrets acquired internally or externally.

4.2 Production Records

4.2.1 The organization shall retain and manage trade secret production records appropriately, ensuring their immutability and authenticity.

4.2.2 If necessary, the organization should entrust the aforementioned trade secret production records to a third-party institution for evidence preservation.

Note: Production records refer to documentation of the trade secret production or the lawful acquisition process, serving to confirm the ownership and source of the trade secret.

4.3 Classification

4.3.1 The organization shall classify its trade secrets.

4.3.2 Assessment factors shall be determined when evaluating trade secret classifications.

Note: Assessment factors can include input costs, economic value, impact of leakage, frequency and scope of use, the organization's confidentiality obligations, etc.

4.4 Confidentiality Period

The organization shall set the confidentiality period based on the content of trade secrets.

Note: When setting the confidentiality period, evaluation factors to be considered can include the life cycle, technological maturity, potential value, and market demand of the trade secret.

4.5 Access Control

4.5.1 The organization shall set access permission for trade secrets according to access needs.

4.5.2 Access permission shall be appropriately managed and adjusted in accordance with employees' employment status, whether currently employed or departed.

Note: Access permission settings can take into account employees' need to know in the course of their business operations.

4.6 Identification

The organization shall ensure that trade secret is clearly identified as such to authorized personnel.

4.7 Management Inventory

4.7.1 The organization shall establish an inventory or database of its trade secrets and regularly review and update it, taking into account aspects such as legal definitions and management requirements.

Note: The management inventory can include trade secrets that are owned solely by the organization, jointly owned with third parties, or obtained from external sources.

4.7.2 The trade secret management inventory shall include the name of the trade secret, its source, time of production or acquisition, and associated control measures.

5. Trade Secret Usage Management

5.1 Separate Management

The organization shall manage the storage, use, and destruction of trade secrets in accordance with their source, classification, and form.

Note: The management of storage, use, and destruction can include backup, external disclosure review, circulation, copy, destruction, etc.

5.2 Backup

5.2.1 The organization shall back up electronic trade secrets and manage the backup data as trade secrets, ensuring their immutability and authenticity.

5.2.2 If necessary, the organization should entrust the aforementioned backup data to a third-party institution for evidence preservation.

5.3 External Disclosure Review

Trade secrets shall only be disclosed externally after review and approval.

5.4 Circulation

5.4.1 The organization shall regulate the circulation of trade secrets, maintain relevant records, and implement tracking management.

5.4.2 When circulating trade secrets, the organization shall ensure that their content is properly protected.

Note: Circulation can include borrowing, carrying out, providing externally, etc.

5.5 Copying

The organization shall regulate the copying of trade secrets, maintain relevant records, and implement tracking management.

Note: Copying can include photocopying, scanning, photographing, printing, and other methods of producing duplicates.

5.6 Destruction

The organization shall regulate the process for destroying trade secrets, ensure that destruction is carried out in a non-recoverable manner, and retain records of the destruction of trade secrets.

5.7 Usage Record Retention

5.7.1 The organization shall retain records of access to and use of trade secrets, ensuring their immutability and authenticity.

5.7.2 If necessary, the organization should entrust the aforementioned records to a third-party institution for evidence preservation.

Note: Usage record retention can include retaining log records from application development systems, database systems, web systems, mail systems, server operating systems, information security equipment, etc.

5.8 Early Warning

The organization shall plan for and review retained usage records, and promptly respond to abnormal usage behaviors of trade secrets.

Note: Abnormal usage behaviors may include large-scale downloading or printing, access at irregular hours, unauthorized email transmission, unauthorized permission changes, etc.

6. Employee Management

6.1 Confidentiality Agreement

The organization shall sign confidentiality agreements with employees who may access trade secrets, ensuring protection of the organization's own trade secrets and reducing the risk of infringing on third-party trade secrets.

Note: The confidentiality agreements can include provisions regarding the scope of trade secrets, ownership, confidentiality obligations, confidentiality period, prohibition of infringement on third-party trade secrets, etc.

6.2 Non-Competition

For employees subject to non-competition obligations, the non-competition clauses in the agreements signed shall comply with applicable legal requirements.

6.3 Disseminations

6.3.1 The organization shall disseminate the group's trade secret management regulations to employees.

6.3.2 The organization shall inform employees that their use of trade secrets will be monitored and that relevant electronic records will be retained.

Note: The organization can use meetings, emails, employee handbooks, employment contracts, slogans, announcements, or training sessions to make employees aware of trade secret management, monitoring, and record retention requirements.

6.4 Education and training

The organization shall regularly conduct education and training sessions to help employees understand relevant trade secret laws and the organization's trade secret management regulations, evaluate the effectiveness of such education and training, and retain related records.

Note: Effectiveness evaluation can be implemented by means of post-training tests (written or oral), post-training reflections, practical exercises, etc., to confirm employees' comprehension of the relevant laws and the organization's trade secret management regulations.

6.5 Discipline and Rewards

The organization shall establish disciplinary regulations for employees who violate the organization's trade secret management regulations, and reward regulations for those who contribute to the protection and management of trade secrets.

6.6 On-boarding Management

6.6.1 The organization shall assess trade secret risks associated with recruitment positions during the recruitment phase and implement corresponding measures.

6.6.2 The organization shall learn about new employees' existing intellectual property and related obligations, and take measures to prevent potential infringement of others' trade secrets.

6.7 Employment Management

During employment, the organization shall review existing confidentiality agreements based on employees' access to trade secrets and determine whether adjustments are needed.

6.8 Resignation Management

6.8.1 The organization shall remind departing employees of their obligations under agreements related to trade secrets, confidentiality, or non-competition, and shall require the return of any trade secrets in their possession.

6.8.2 For key departing employees, a trade secret protection interview shall be conducted. If the interview cannot be conducted for any reason, a written notice shall be provided, and records shall be retained.

6.8.3 If necessary, the organization should investigate whether departing employees have engaged in abnormal trade secret usage.

Note: Investigation methods can include reviewing employee log records, conducting anomaly analysis, inspecting employee computer equipment, etc.

6.8.4 The organization shall conduct follow-up tracking of key employees after their departure.

7. Network、Environment and Equipment Management

7.1 Area Control

The organization shall plan control actions for areas where trade secrets are retained or processed, including access control for personnel, and retain relevant control records.

Note 1: Personnel include employees as well as personnel from external entities.

Note 2: Control actions can include requiring employees to wear identification badges, installing physical barriers around office areas, implementing visitor management systems, using alarm systems, automatic locking doors, or deploying security personnel, etc.

7.2 Surveillance Equipment

The organization shall install surveillance equipment in key controlled areas and related critical facilities.

7.3 Equipment Control

7.3.1 The organization shall exercise control over recording media and information equipment containing trade secrets.

7.3.2 If necessary, the organization should control the carrying in, carrying out, and use of recording media or information equipment with photographic, video recording or audio recording functions.

7.4 Network-Related Control

7.4.1 The organization shall manage network security for the access and transmission of trade secrets.

Note: Network security management may include firewall protection for computer networks, remote access control, email transmission control, segregated storage of trade secrets on separate servers, software installation restrictions, and limitations on the use of network communication software or cloud services outside the scope of corporate supervision for transmitting or accessing trade secret data, etc.

7.4.2 The organization shall control remote access to trade secrets.

8. External Activity Management

8.1 Confidentiality and Ownership Agreements

8.1.1 Before providing trade secrets to external entities, the organization shall execute written agreements with them to ensure the protection of its own trade secrets and to reduce the risk of infringing on others' trade secrets.

Note: External entities can include outsourcing and procurement partners, such as upstream providers, outsourcing vendors, collaborative R&D partners, as well as patent and trademark firms and law firms that provide IP management-related services, such as litigation, patent application, patent analysis, trademark registration, and infringement assessment.

8.1.2 If necessary, the organization shall sign agreements with external entities involved in intellectual property output regarding the ownership of derivative rights.

8.2 External Provision of Trade Secrets

8.2.1 When providing trade secrets externally, the organization shall require external entities to maintain confidentiality and provide proof of receipt of the trade secrets.
8.2.2 If necessary, the organization should take measures to ensure that external recipients of trade secrets no longer keep such trade secrets after its intended use is complete.

8.3 Requirements for External Entities

8.3.1 The organization shall establish selection criteria for external entities regarding trade secret protection and management capabilities, and conduct assessments.

Note: Regarding trade secret protection and management capabilities, the organization can consider factors such as the design completeness and operational implementation of the external entity's trade secret management system, any history of leakage disputes, etc.

8.3.2 If necessary, the organization should investigate the trade secret management capabilities of external entities.

9. Dispute resolution

9.1 Dispute resolution Mechanism

9.1.1 The organization shall establish a trade secret dispute resolution mechanism to prevent or mitigate damages to the organization and to ensure that top management is adequately informed and assisted in making decisions.

9.1.2 The TS dispute resolution process shall include at least the following: confirmation of the infringed subject matter, collection of relevant evidence, and sealed custody.

Note: Relevant evidence can include information about suspected offenders, possible leakage channels (such as server logins, email transmissions, paper printouts, transmission or photography with information equipment, malicious poaching, competitors purchasing at high prices), specific facts of infringement, etc.

10. Monitoring and Improvement

10.1 Monitoring

10.1.1 The organization shall verify the implementation status of trade secret management to determine whether it meets the following requirements:

(a) Compliance with the requirements of this document;

(b) Compliance with the management policies and objectives established by the organization;

(c) Effective implementation and maintenance.

10.1.2 Regarding the aforementioned verification, the organization shall ensure that:

(a) the impartiality of the process and the objectivity of the results;

(b) the verification results are reported to relevant management;

(c) appropriate corrective and improvement actions are taken in a timely manner.

10.2 Improvement

The organization shall use appropriate methods to evaluate whether there are areas of the trade secret management system that can be continuously improved, and take necessary corrective and improvement actions.