Management Guidelines for Trade Secrets

January 30, 2003

(Last update: March 31, 2025)

Ministry of Economy, Trade and Industry

Record of revisions

Revised: October 12, 2005
Revised: April 9, 2010
Revised: December 1, 2011
Revised: August 16, 2013
Revised: January 28, 2015
Revised: January 23, 2019
Revised: March 31, 2025

Table of contents

Introduction (The Nature of the Guidelines)

○ **Characteristics of the Guidelines**

・ The Guidelines, established by the Ministry of Economy, Trade and Industry, specify a set of concepts that it has from the viewpoint of an administrative organ in charge of the Unfair Competition Prevention Act (referred to as "the Act" below) and of managing trade agreements, including the TRIPS Agreement (Agreement on Trade-Related Aspects of Intellectual Property Rights). The Guidelines address the definitions and other details of trade secrets, including requirements for protection under the Unfair Competition Prevention Act, based on the goal of promoting innovation, changes in working and employment style, overseas trends and typical court decisions both at home and abroad (although no decisions have yet been given by the Supreme Court of Japan on these issues as of the current revision of the Guidelines), along with other aspects. The Guidelines, however, are not legally binding.

・ Naturally, specific issues concerning the Unfair Competition Prevention Act are eventually decided in the courts.

○ **History of revisions**

・ The Management Guidelines for Trade Secrets[1], which were established in January 2003 as reference Guidelines to enable corporations to establish strategic programs to reinforce their management of trade secrets, were fully revised in 2015.

・ For the full 2015 revision, based on the 2014 Intellectual Property Promotion Program (decided by the Intellectual Property Strategy Headquarters in July 2014), which states that "we will revise the Management Guidelines for Trade Secrets to be legally recognized as such, thereby specifying them in manners easier for business operators to understand, taking account of the opinions raised in some court decisions that the criteria for secrecy management is considerably strict and unpredictable," deliberation was undertaken by the Subcommittee on the Protection and Use of Trade Secrets, the Intellectual Property Subcommittee and the Industrial Structure Council (referred to as "Trade Secrets Subcommittee" below).

・ After that, in view of the degree to which the use of data diversified as a result of the advent of the Fourth Industrial Revolution which incorporates the use of big

[1] The guidelines were revised four times according to the growing stock of court decisions and amendments of the Unfair Competition Prevention Act, until January 2015.

data and artificial intelligence, the Trade Secrets Subcommittee held its debate and presented its decided method of reviewing the Management Guidelines for Trade Secrets based on the market realities of how trade secrets are protected (Study of the Unfair Competition Prevention Act in View of the Fourth Industrial Revolution announced in May 2017: an Interim Summary[2]), and accordingly these Guidelines were partially revised in January 2019.

- In addition, the Unfair Competition Prevention Act amended in 2018 in relation to the protection of shared data with limited access came into effect in July 2019, and the Unfair Competition Prevention Act amended in 2023 to exclude trade secrets from the scope of protection of shared data with limited access came into effect in April 2024. Prior to the enforcement of the amended Act, the "Guidelines on Shared Data with Limited Access" were revised in February 2024[3].

- Furthermore, while workplaces were traditionally limited to corporations' facilities, many corporations have begun adopting teleworking in response to recent circumstances, and opportunities for working outside the corporations' facilities are increasing; as a result, opportunities to come into contact with trade secrets at home and other places are also increasing. Not only employees within a corporation but also temporary workers dispatched based on contracts between a corporation and a dispatching agency now have more opportunities to come into contact with trade secrets. With the trend toward diversification of working styles, there has been a rise in concurrent employment and side jobs, which leads to opportunities for employees to come into contact with trade secrets at their concurrent or side jobs. At the same time, with regard to information management methods, management based on cloud technology and environment is advancing, and the way information is managed within a corporation is also changing.
  In light of these trends, some parts of these Guidelines were revised in March 2025, along with some rhetorical changes.

○ **Management level indicated in the Guidelines, etc.**

- The Guidelines present the minimum level of measures necessary to receive legal protection as defined under the Unfair Competition Prevention Act, including

---

[2] https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/eigyo_himitsu/pdf/20170509001_1.pdf

[3] Guidelines on Shared Data with Limited Access are available at: https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_shared_data_with_limited_access.pdf

filing for injunctions and damages as subsequent remedies in cases where trade secrets among diverse information held by a corporation, etc. have been wrongfully acquired, etc.

- With regard to information held by corporations, universities and research institutes, it is desirable to take, in addition to the measures indicated in the Guidelines, comprehensive measures and security measures (including advanced measures) recommended to prevent leakage of trade secrets or in the event of leakage that go beyond the measures indicated in the Guidelines regarding various kinds of information in general that need to be managed as confidential, such as trade secrets for which appropriate management is required as a prerequisite for legal protection, but the necessity of management is left to the discretion of the holder or information for which the holder is required by law to take certain management measures, etc.[4] For such security measures, see the Handbook for Protecting Confidential Information[5].

- The Unfair Competition Prevention Act was amended in 2018 to introduce protection for shared data with limited access, which protects trade secrets and information and data held by corporations in a mutually complementary manner. For details on the protection of shared data with limited access, see the Guidelines on Shared Data with Limited Access (https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_shared_data_with_limited_access.pdf).

---

[4] Such as personal information subject to the Act on the Protection of Personal Information and important technical information subject to the Foreign Exchange and Foreign Trade Control Act.

[5] *Handbook for Protecting Confidential Information* is available at:
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf
Moreover, *Guide to Handbook for Protecting Confidential Information*, compiled as a digest of said book, is available at:
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/170607_hbtebiki.pdf
In addition, the following educational material, "Things about Trade Secrets You Should Know About to Stay Out of Trouble!," organizes points to keep in mind from the perspective of the Unfair Competition Prevention Act for employees who are engaged in business at corporations, etc. and are in a position to actually come into contact with trade secrets:
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/shitteokitai_eigyohimitsu.pdf

1. General

○ **Characteristics of the Unfair Competition Prevention Act**

・ The Unfair Competition Prevention Act prohibits, as unfair competition, such acts that illicitly take advantage of the results of another party's technical development, product development, or other effort. More specifically, the Unfair Competition Prevention Act provides civil remedies, including injunctions and damages against acts of wrongful acquisition, use and disclosure of trade secrets alongside use of a brand indication or symbol, provision of goods that imitate the shape and/or configuration and similar operations, and the said Act is characterized as subject to extraordinary rules of the Tort Law.

○ **Definition of trade secrets under the Unfair Competition Prevention Act**

・ Article 2-6 of the Unfair Competition Prevention Act (referred to as "the Act" below) defines trade secrets as technical or business information that is:

1) kept secret (secrecy management)
2) useful for business activities, for example methods of manufacturing or marketing (usefulness)
3) not publicly known (non-public domain).

All three requirements are necessary in order to secure legal protection.

・ Also note that the protection provisions for trade secrets in the Act, including these three requirements, are so characterized as to ratify the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS, which, based on negotiations conducted beginning in 1987, Japan joined in 1995), which stipulates minimum standards of protection for intellectual properties for members of the World Trade Organization (WTO). In interpreting the Act, one should consider the existence and content of TRIPS. It is to be noted that virtually the same three requirements as above are set as criterion for protecting trade secrets in other countries as well (but there are some differences in the enforcement of such Acts).

[Reference] Text of TRIPS (excerpts)

SECTION 7: PROTECTION OF UNDISCLOSED INFORMATION

Article 39

1. In the course of ensuring effective protection against unfair competition as provided in Article 10*bis* of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.

2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices, so long as such information:
(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
(b) has commercial value because it is secret; and
(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

○ Relationship between trade secrets, and civil measures /criminal penalties

- Any issue falling under the category of trade secrets can be subject to civil remedial measures, including injunctions and criminal penalties, under the Act.

- The interpretation of the three requirements, such as secrecy management, is considered to be the same both in civil and criminal cases[6].

- It is to be noted that even if, however, the three requirements, including measures to maintain secrecy, are recognized and the information falls under the category of trade secrets, it is necessary to satisfy all the requirements for "unfair competition" and "trade secret infringement" under the Act (such as Articles 2-1-4 to 2-1-10, and Article 21-1) to be subject to injunctions and other civil measures and criminal penalties.

○ Protection of information by means other than trade secrets

- Although information not falling within the category of trade secrets cannot be protected as a trade secret under the Act, such information may be eligible for protection as shared data with limited access under the same Unfair Competition Prevention Act (Article 2-7) or other laws and regulations.

- For example, if the information does not fall under the category of trade secrets but falls under the category of shared data with limited access, it may be possible to demand an injunction based on the shared data with limited access, etc.[7]

---

[6] "Even in criminal measures, in light of the circumstances surrounding the 2003 amendment of the Unfair Competition Prevention Act, the requirement of whether it falls under the category of trade secrets is considered to be the same as that in civil measures." [Decision by the Nagoya District Court, March 18, 2022; 2017 (Wa) 427]

[7] It is to be noted that, just like trade secrets, even if data falls under the category of shared data with limited access, it is necessary to satisfy all the requirements of "unfair competition" under the Act (Article 2-1-11 through 2-1-16) to be subject to civil measures such as injunctions.

- If a separate set of regulations are established under an agreement between individuals regarding the handling of the information, it may be possible to file for injunctions or other measures under the agreement. At that time, the issue of whether the case falls under trade secrets under the Act is basically not deemed relevant.

○ Relationship with information management at organizations other than corporations, such as universities and research institutes

- Although the Guidelines are intended for private corporations, such as "corporations" and "employees," the content is also highly applicable to the management and protection of trade secrets at universities and research institutes.

- Some valuable research results have value for universities and research institutes when managed as confidential information in the same way as private corporations, and thereby they become information that falls under the category of "trade secrets" covered by the Unfair Competition Prevention Act[8]. For this reason, it is highly possible that universities and research institutes possess "trade secrets."

- In fact, there are court decisions that assume universities to be included in the definition of "businesses" under the Unfair Competition Prevention Act[9], and there has been a case where taking out (leakage to an outside party) information that was deemed to fall under the category of trade secrets by a researcher working at a research institute became an issue as a violation of the Unfair Competition Prevention Act. Universities and research institutes may therefore be considered to fall under the scope of the Guidelines.

[8] Among information held by universities and research institutes, not only external confidential information provided by private corporations participating in joint research but also research and experimental data generated and held by universities and research institutes fall under the category of "trade secrets" covered by the Unfair Competition Prevention Act.

[9] Decision by the Tokyo District Court, July 19, 2001; No. 1815, p. 148

2. Secrecy management

(1) The spirit of the secrecy management requirements

The spirit of the secrecy management requirements is to provide predictability to employees[10], officers, and external partners (referred to as "employees" below) by specifying for which items within a specific corporation employees are to maintain confidentiality (the scope of information), thereby ensuring stability in business practices

○ **Characteristics of trade secrets as information**

- Information itself is intangible, and owned and managed in various ways, and defining trade secrets cannot be based on the premise that they should be published as in the case of patents and related rights. It is therefore possible that employees who acquire, use, or disclose such information are unaware that a particular piece of information constitutes a trade secret protected under the Act.

○ **The spirit of the secrecy management requirements**

- The spirit of the secrecy management requirements is to prevent someone who has come into contact with the relevant trade secret from being unexpectedly suspected of a crime ex post facto, and to provide predictability for employees by specifying for which items within a specific corporation the employees are to maintain confidentiality based on the nature of such trade secrets, thereby ensuring stability in economic activities[11].

○ **Important notice**

- It is not appropriate to require that a specific corporation implement high degrees of security measures regarding a piece of information in order to receive legal

[10] Including dispatched workers under the Act on Ensuring the Proper Operation of Worker Dispatching Services and Protecting Dispatched Workers from the perspective that they engage in work based on directions and orders from their clients.

[11] The premise is that as the legal requirements indicate, inappropriately managed information will sooner or later come to be known by rival companies, resulting in a loss of competitiveness for the holder of the information. Consequently, giving legal protection to such information cannot incentivize research and development. Therefore, it can be said that the secrecy management requirements are not for the less-managed information but for the reasonable independent efforts of the particular company to control certain information as a set of secrets (for example, Yoshiyuki Tamura, Changes in and the Appropriateness of Court Decisions Regarding the Secrecy Management Requirements for Trade Secrets – Subjective Awareness vs. *Objective* Management --, *Intellectual Property Management* vol. 64, 5 and 6). In that sense, the Guidelines mainly explain the principle of predictability for employees and are different from the opinion mentioned above.

protection under the Act. Here are the reasons[12]:

- In real-world economic activities, benefits of trade secrets are mostly realized by being shared and used systematically both inside and outside the corporation that owns them. Some corporations need to share their trade secrets with their subsidiaries, affiliates, or outsourcing partners, or with universities and other research institutes through industry-academia collaboration in various locations both at home and abroad. Effective and efficient security measures should therefore be maintained in accordance with the level of risks and the costs for measures.

- The number of corporations, particularly SMEs, where trade secrets can be a source of competitiveness is on the rise. It is not realistic to expect these corporations to implement impregnable security measures, which would result in hampering innovation.

- Should subcontractor information, private information, or other trade secret be leaked, the victims would not always be limited to the legitimate trade secret holders.

(2) The necessity of the secrecy management measures

For secrecy management requirements to legally satisfy the definition, it is necessary that the intent to maintain confidentiality within a specific holder regarding a specific, legally owned trade secret has been clarified to its employees by using appropriate confidentiality measures, thereby allowing the employees and other workers to recognize the said intention of confidentiality. The required contents and levels of specific security measures vary with the size and business style of specific corporations, the responsibilities of the employees, the nature of the information and other circumstances, and the security measures should be generally and easily understood by employees in the managerial units of the corporations (see page 19 of the Guidelines).

[12] Another policy statement holds that despite the presence or lack of a security measures, information that an employee has acquired with the knowledge that the same is a secret of his/her employer (the employer wants to keep it a secret) should be acknowledged as a trade secret, and the employee should therefore be subject to civil measures/criminal penalties. This, however, does not necessarily fit the statement in the current Act that "that is kept secret" and, if such an idea is employed, any ruling or decision will depend on the fact of an employee's implicit knowledge at the time, which is difficult to verify after the fact. This situation is therefore considered to have low predictability, and to risk hampering stability in economic activities, or smooth job-changing of an employee.

○ **General**

・ For the security requirements to be satisfied, it is not enough for only holders of trade secrets to be aware of the relevant information as secrets.

That is, it is necessary to indicate clearly to the employees the intention of the holders of trade secrets to manage their secrets (the intention to manage specific information as secrets) by means of rational and economically feasible secrecy management measures[13] according to specific circumstances, thereby allowing the employees to easily discern the said intention to manage the secrets (in other words, recognition of the intention is ensured).

Trade partners should be informed of the intent to maintain the secrecy of trade secrets in substantially the same manner as the employees.

○ **Those subject to secrecy management measures**

・ Those subject to secrecy management measures are employees and other workers who can legally and actually come into contact with the information.

This essentially refers to people who can actually come into contact with trade secrets, including those who can legally come into contact with the information, although it is unclear whether the contact is within the scope of their professional responsibilities or not (for example, workers delivering information between departments, or employees from other departments in cases where they can access unlocked book vaults in a large room shared by many employees).

The secrecy management requirements should be determined objectively, including the level of awareness of all employees, and are not affected by how

[13] For secrecy management requirements, jurists have conventionally explained that the following two items serve as determining factors: 1) that a limit is imposed on those given access to specific information (restricted access); and 2) that provisions are in place to allow those who have accessed the information to recognize that it is a trade secret (recognizability). However, although both are important factors in judging whether items are to be kept confidential, they are not mutually dependent requirements. “Restricted access” can be considered as a means of ensuring “recognizability.” If, therefore, those accessing the information can recognize that it is secret (it satisfies the “recognizability” requirement), the attempt to maintain secrecy will not be denied on the grounds that there are not enough barriers to access (see the decision by the Tokyo High Court on March 21, 2017; Hanrei Times No. 1443, p.80).
If, however, the employees or other workers in question actually understand that a certain item of information is confidential, it is not the case that secrecy management measures are completely unnecessary on the part of the trade secret holder. In view of the fact that the Act does contain a provision that says that the Act applies to information “that is kept secret" (Article 2-6 of the Act), the secrecy management requirements are unmet when no secrecy management measures are taken.
It is to be noted here that the term “restricted access” is mostly used to mean that measures should be taken to prevent unauthorized personnel from gaining access to the relevant information. It is, however, appropriate to include measures for keeping any information secret in a broad sense, including “labeling it as a secret” and “contractual measures under confidentiality agreements or similar contracts.” To clarify this distinction, the Guidelines explain it by using not the term “restricted access”, but the term “secrecy management measures.”

individual employees have actually understood them[14].

- The mere existence of secrecy management measures for employees ensures secrecy management against intruders and similar offenders (those trying to obtain trade secrets through fraud or similar actions as defined in Articles 2-1-4 and 21-1-1, such as those in contact with information by an act falling under the category of intruding into a residence). This therefore does not need to be stipulated in the clause for intruders and similar offenders (that is, another secrecy management measure does not need to be taken) separately from the case of the intention of the holder of the trade secret to manage its secrecy for its employees.
  *Criminal punishment of intruders needs to satisfy, in addition, the requirements of deliberateness and the purpose of wrongful gain or causing damage.

○ Degree of **secrecy management measures**

A. For employees and officers

- Secrecy management measures to be required include, mainly, selecting a medium, labeling the relevant medium, limiting the number of persons able to come in contact with the relevant medium, separate management of trade secrets and other information[15], listing the types and categories of trade secret information, specifying confidentiality obligations in rules, etc. such as employment rules and confidentiality agreements (or written oaths) or other documents, and training and awareness-raising for employees. In short, the point is that the efforts (management measures) to be made should be important enough to raise an awareness of norms that for employees, who are subject to such secrecy management measures, the fact that the relevant information is a secret and should be handled differently from general information is understood.

- The specific contents and degree of secrecy management measures vary with the number of employees in contact with the relevant trade secrets, the business style, the occupations of the employees, the nature (importance) of the information, the circumstances of offices, such as layout, and other circumstances.

  - For example, with regard to the nature of the information, if it is clear to employees that the information is important to the trade secret holder and must

[14] Decision by the Intellectual Property High Court, June 24, 2021; 2020 (Ne) 10066

[15] For information on the separate management of trade secrets and other information, see the "Handbook for Protection of Confidential Information" ("Restricting Access to Information through Separate Storage" on page 45 onward of February 2024 revised edition) referred to in Note 5, which provides specific management methods as examples of measures to prevent information leakage.

obviously be managed as confidential, management utilizing such employees' awareness should be permitted[16], and in some cases, it may be sufficient if technical measures such as restricting access to confidential information by requiring IDs and passwords to log in to corporations' computers or normative measures such as prohibiting the leakage of such information in employment rules and written oaths[17] are taken.

- With regard to limiting persons who come into contact with the media in question, it is not required to strictly limit access on a per-employee basis after considering the necessity of their work, and even if the access rights are widely granted in a specific department due to operational necessity, etc., it can still be considered that the access is limited to specific employees[18].

- If the number of employees that can come into contact with trade secrets legally and practically is small, taking simple measures such as oral checks for "confidential information" may be sufficient between the relevant employees.

Important notice

- If the secrecy management measures for information are substantially weakened to the point that they are no longer effective, and if the employees cannot easily discern the relevant corporation's intent to manage its secrets, then the secrecy management measures cannot be deemed appropriate[19].

  *Note: It is not appropriate to label security measures as "losing substance" in the case of a temporary or accidental instance of careless management that does not seriously affect the employees' ability to recognize the relevant corporation's intent to manage its secrets.

- Personal information protected under the Act on the Protection of Personal Information seems more likely to satisfy the requirement of secret management than other information. This is because the said Act obligates corporations that own

16 See the decision by the Intellectual Property High Court, September 27, 2011; 2010 (Ne) 10039, and the decision by the Tokyo District Court, December 9, 2022; 2021 (Toku-Wa) 129, etc.
17 See the decision by the Osaka District Court, March 5, 2018; 2016 (Wa) 648.
18 See the decision by the Fukuoka High Court, July 3, 2024; 2024 (U) 20.
19 It should be noted that even if confidentiality labels, etc. are in place in ways such as "all information learned in the course of duties" or "all information within the office," if the information contains a significant amount of information that employees naturally recognize as general information based on the content thereof, it may be evaluated as "secrecy management measures have lost their substance."

the personal information to manage the safety of the personal information, including leakage prevention, because it is clear to employees as well, and because such information can clearly be distinguished from general information in terms of appearance.

- Preventive measures against information leakage, subject to the specific corporation's own discretion, commonly include measures to reduce the risk of leakage by raising awareness levels[20] of employee behavior in line with the magnitude and other characteristics of the risk of leakage; measures to reduce the risk of leakage by conducting checks, engaging in preemptive detection of leaks, and other measures; or measures to prevent the spread of damage. It is important to highlight that these measures are not identical to the legally recognized secrecy management measures and so do not provide the same avenues for legal recourse.

- With regard to information security, although it is important to take necessary measures according to the circumstances of each corporation from the perspective of reducing the disadvantages it may suffer, the degree of measures required for information security and the degree of secrecy management measures can be different, and secret management measures may be acceptable even if they do not reach the degree of measures required for information security.

Typical court decisions for reference

- **An example decision based on the size of the company**

  The court affirmed secrecy management despite the fact that the relevant company did not limit access with passwords or other means, and affixed no labels indicating that the information provided was confidential, considering the facts that the company only had a total workforce of 10 and the recognition of the intention was ensured, and the company was unable to limit everyday access to the unique information without hampering their business operations. [Decision given by the Osaka District Court, February 27, 2003; 2001 (wa) 10308].

- **An example where lenient management was deemed acceptable because of the needs of the business**

  The court affirmed secrecy management when employees kept the relevant client

[20] A desirable way to raise employee awareness would be to take platforms for labor-management dialog, training on information management rules and similar matters, e-learning and other training programs, and various other opportunities to inform all employees of what trade secrets are, the importance of trade secrets that the employees handle, the permissible scope of sharing, the periods during which to keep the trade secrets, and other issues.

information easily recognizable as confidential, despite the fact that employees distributed copies of client information to superiors and other personnel, brought them to their private homes, kept records of the information in notebooks and, even after completing the business dealings with the client in question, kept the notebooks based on the needs of the business. [Decision by the Intellectual Property High Court, July 4, 2012; 2011 (ne) 10084].

・**An example of a decision that the information is, by nature, recognizable by the employees**

Information about the technology for manufacturing PC resin is rare, and the employees involved in its manufacture can be said to have been aware that the said manufacturing technology was confidential. The court therefore affirmed its secrecy management [Decision by the Intellectual Property High Court, September 27, 2011; 2010 (ne) 10039].

・**An example of a decision that the information is recognizable by employees in light of the importance of the information in addition to normative management being in place**

The court affirmed secrecy management, considering that despite the fact that the degree of access restriction is unclear and it is difficult to say that physical management was thoroughly implemented, the normative management was implemented by integrating customer information and managing it by way of data management and by prohibiting the disclosure of customer information in the employment regulations and requiring former employees to sign an agreement promising not to leak customer information, and it was also easy for the employees to recognize that customer information should be subject to secrecy management in light of the importance of customer information for household distribution operators [Decision by the Osaka District Court, March 5, 2018; 2016 (wa) 648].

・**An example of affirming secrecy management without putting physical management at issue**

The court affirmed secrecy management in view of the importance of the relevant confidential information based on the facts that the information enables extremely effective business activities including acquiring low-price transactions, the information was disclosed to only 11 persons, and that immediately before the defendant resigned, the company had caused the defendant to submit a written oath of confidentiality, among other circumstances [Decision by the Osaka High Court, July 18, 2008; 2008 (ne) 245].

B. For trade partners

・ If confidential information is provided to trade partners, it is important to confirm whether the information was provided after concluding a confidentiality agreement with the trade partners, in addition to implementing secrecy

management measures for employees and officers[21].

(3) Specific examples of secrecy management measures

Secrecy management measures, as described in (2) above, vary with specific circumstances. Here, let us take one example and introduce you to a typical set of secrecy management measures.

*Note: Secrecy management methods are not limited to measures targeting the recording media itself, but also those which limit access to the information to authorized personnel. In addition, intangible information can be managed as secret information.

1) Printed documentation

○ Typical management method

・ For example, labeling documents containing confidential information as "Confidential" or otherwise secret, will presumably ensure that employees recognize the company's intention of maintaining secrecy.

・ In addition, another conceivable method of ensuring recognition of confidentiality is simply storing such information in a lockable cabinet, safe, or similar container or room.

・ It is to be noted that when the risk of unauthorized acquisition of information is obvious, for example in a case where information leaks occur frequently within a company, it is conceivable that a ban on photocopying, scanning, and photographing of information on paper, placing controls on the numbers of copies to be made (the shredding and discarding of excess copies), the collection of previously distributed copies, the locking of cabinets, a ban on removing the information from the premises, and other additional measures may further reinforce the company's explicit intention to maintain the secrecy of the information. Under normal circumstances, these measures may be effective in preventing information leaks, but they do not necessarily satisfy the secrecy management legal requirements. [As described in (2) above, corporate decisions to take more advanced, voluntary information leakage measures to reduce the risk of leaks do not necessarily fall within the definition of secrecy management].

[21] However, concluding no confidentiality agreement with the other party does not necessarily mean that secrecy management has been inadequate, and it can be considered that disclosing trade secrets to the other party without concluding a confidentiality agreement in advance does not immediately constitute a failure to take secrecy management measures.

Typical court decision for reference

・ An incident occurred where an employee of a personnel-dispatching agency removed information and other material concerning the employment contracts of its temporary workers. The relevant information was not stored in lockable cabinets, photocopying was not restricted and collection of photocopies was not mandatory, and no confidentiality labels were affixed to the documents. The court, however, affirmed secrecy management in view of the facts that the agency had given its employees, including the offending employee, general warnings and other instructions concerning their confidentiality agreement and the management of the relevant information [Decision by the Tokyo District Court Decision, December 26, 2002; 2000 (wa) 22457].

2) Electronically stored information

○ Typical method of management

・ Information stored as digital data or in an electronic format is basically treated in the same manner as printed information. Secrecy management measures for electronic information are considered adequate when any of the following methods are employed:

- Attach confidentiality labels to recording media.

- Mark electronic files and folders as confidential.

- Mark the electronic data in the relevant electronic file as confidential (by means such as marking the header of each such document file as confidential) so that a message to the effect that the information contained in the file is confidential will be displayed when an electronic file containing a trade secret is opened.

- Employ password protection for electronic files that contain a trade secret, or for folders containing such electronic files.

- If it is impossible to affix a label to the recording medium itself, attach a “Confidential” label to relevant device cases (such as CD cases) or other containers.

・ Storing and controlling a trade secret using an external cloud service is also applicable, if it is managed as a secret. One conceivable method is imposing hierarchical control restrictions. If the content or nature of the information clearly indicates that the information is important for the trade secret holder, it may be

sufficient if technical measures such as setting IDs and passwords to access external clouds or normative measures such as prohibiting the leakage of such information in employment rules and written oaths are taken.

・ If the risk of wrongful use or unauthorized acquisition is significant, one conceivable security measure is to change passwords with every change in personnel, to limit the forwarding of emails to private email addresses by changing mailer settings, to physically disable USB or Smartphone connectivity, or make other changes, thereby reinforcing the corporation's ability to maintain secrecy. Under normal circumstances, however, although these measures may be effective in combatting information leakage, they are not necessary to satisfy the legal secrecy management requirements. [As described in (2) above, corporate decisions to take more advanced, voluntary information leakage measures to reduce the risk of leaks do not necessarily fall within the definition of secrecy management].

Typical court decisions

・The court affirmed secrecy management even though multiple employees had shared an ID and a password for an information-containing PC, had the ID and password written on a label attached to the outside of the PC, and even after the ID and password remained unchanged after one of those people left the company. The court stated that there was no reason to deny secrecy management, unless the ID and password were completely meaningless [Decision by the Osaka District Court Decision, June 12, 2008; 2006 (wa) 5172].

・One employee had never changed his password and even had the password written on a tag attached to his PC. In an incident where it was not agreed that printed price lists would be stamped to the effect of their being confidential or secret, the court affirmed the secrecy management of the responsible company which did not tolerate the practice of presenting and taking the price lists to outside parties, in view of the fact that the price lists indicated purchase costs and other information, which are in general clearly important to machine manufacturers [Decision by the Nagoya District Court, March 13, 2008 (wa) 3846].

3) When a product itself is a trade secret

・ For manufacturing machines, molds, highly functional microorganisms, new product prototypes, and other items that themselves constitute trade secret information, but due to their nature cannot preclude confidentiality labels or being stored in safes or vaults, they can presumably be subject to secrecy management measures by using any of the following methods:

- Signs affixed to doors or near entrances, saying “Authorized Personnel Only”.

- Employing security personnel or installing gates or other barriers activated by appropriate credentials, thereby controlling the access of unauthorized personnel to the factory.

- Attach signage prohibiting photography.

- Create a list of the trade secrets, and allow employees who could potentially come into contact with any of the commodities, products or properties based on the trade secrets, to have access to the list.

4) When no medium is used

・ For example, for intangible know-how that an employee has learned involving skills, design, or anything similar, and customer information and similar data that an employee has memorized as part of his job responsibilities, it is necessary as a rule to record the details thereof on paper or other medium in a manner similar to those shown below, in order to provide employees with predictability and freedom to choose future employment (*1) [the management of such information once committed to a particular media is described in 1) to 3) above].

- List the categories of trade secrets (*2).

- Specify the trade secrets in a document or something similar.

*Note 1: Trade secrets are often difficult to distinguish from general information. Prohibiting their use without displaying the relevant information makes it unclear to employees what kind of information they are prohibited from disclosing or removing from the office. This, then, may make it difficult for them to change jobs.

*Note 2: A typical example is an organization that develops leading-edge technologies. In environments where advanced trade secrets are created and developed every day and are not constantly organized or classified, it is presumably effective to determine the scope of such developments by creating lists of relevant categories and establishing confidentiality agreements (or written oaths), or something similar.

・ On the other hand, if for example, such trade secrets involve particular reaction

temperatures, reaction times, trace elements, or the mix ratios of two or more substances (often seen in the chemical and similar industries), or as-yet unpatented or unregistered discoveries, but if the scope of trade secrets is clear to the employees in the company due to the particular circumstances of the company including the limited number of employees, the nature of the information, and other relevant trade secrets, then - even if the details themselves are not displayed – the employee's ability to recognize secret information can be ensured by telling employees the scopes and categories of the relevant items of information.

・ Using or disclosing information that was a trade secret of their previous employer after a job change does not necessarily and immediately make them subject to civil measures/criminal penalties. The employee will only be subject to civil measures/criminal penalties if there has been a considerable violation of the principle of good faith in light of the benefits to the relevant company, the benefits to the employee, the contents of the trade secret, etc., in other words, if it is considered to be used for the "purpose of wrongful gain" or the "purpose of causing damage to the holder."[22].

5) When the trade secret is recorded on two or more distinct media

・ The same information is often controlled in paper and electronic formats in corporate practices. In managing the same trade secret in two or more media formats, however, each individual format is, as a rule, subject to secrecy management measures.

・ However, if an employee may be in contact with the information in more than one medium, and if the company's intent to keep the relevant information secret is recognizable due to secrecy management measures (such as confidentiality labeling) for either medium, then, even if the company's intent to keep the information secret is difficult to discern with one medium, it is the norm to assume that secrecy management is maintained.

(4) Concept of secrecy management when a trade secret is shared with various offices or operational locations either internal or external to the company or both

When a trade secret is shared both inside the company (with branches or stations)

[22] If after a job change, the retiring employee discloses a trade secret or something similar to their new employer in a manner considerably violating their obligations in terms of the principle of good faith in their relations with their former employer, the new employer would be infringing on a trade secret if they used or otherwise handled the trade secret in bad faith or through a serious mistake with regard to a disclosure considerably violating such obligations in terms of the principle of good faith.

and outside it (with subsidiaries, affiliates, suppliers, outsourcing vendors, franchisees, or other entities), the information is organized as follows:

1) Cases where the same information is owned at more than one location, but internal to the company

Secrecy management or the lack thereof is not determined by the entire company, but by each independent unit that controls information as trade secrets (hereafter, "control unit"). To employees within the said control unit, it is enough for there to be recognizability of secrecy management measures within the said control unit.

- If people own the same trade secret at more than one location within the company, for example at different branch offices, each location should take secrecy management measures appropriate to the circumstances. If, however, no secrecy management measurements are taken at one of the locations (despite the fact that at the relevant location the court would reject a secrecy management claim), it does not mean that the secrecy management claim for the relevant information is also denied at other locations.

- That is, it is enough for there to be recognizability of the company's intent to maintain secrecy for each control unit (a unit considered to have a certain degree of independence regarding the control of trade secrets due to the size, physical environment, and business details of the unit, along with decisions on the necessity and content of secrecy management measures, the existence or lack of autonomous decision authority to supervise their observance status (such as dispositions for violators), and the existence or lack of other circumstances within the unit. Such units are typically "branches" and "divisions").

*Note 1: If information leaks from control unit A, which is equipped with adequate secrecy management measures, then a lack of secrecy management measures in control unit B usually does not negate the secrecy management status of control unit A. If, however, the lack of secrecy management measures in control unit B is continuous and is a known fact in the company, meaning that control unit A's secrecy management status also lacks recognizability for control unit A's employees, then if information subsequently leaks from control unit A, secrecy management status within control unit A may be rejected by the court (but this does not mean that temporary or accidental imperfect management within a specific unit will immediately damage secrecy management status).

*Note 2: In the case where information α managed as confidential in control unit C is used for generative AI[23], even if information α is subsequently generated and output from the generative AI in control unit C as an AI product, as long as information α is managed as confidential in control unit C, it is considered that the secrecy management in control unit C will not be denied solely on the basis that information α was generated and output in control unit C[24]. Also, even if information α is generated and output from the generative AI in control unit D as an AI product, as long as information α is managed as confidential in control unit C, it is considered that the secrecy management in control unit C will not be denied solely on the basis that information α was generated and output in control unit D.

2) Cases where two or more companies share the same information

As the existence or lack of secrecy management is determined by each company (more specifically, each control unit), the specific control status of information within another company does not as a rule affect the secrecy management within the home company.

- **Decisions made by independent companies**

  For other corporations, corporate law and similar regulations seem to assume that the holder owning trade secrets itself cannot take or ensure secrecy management measures directly within such other partner corporations. In addition, the Act uses the concept of the "holder," and stipulates that management is performed on an operator-by-operator basis. The specific control status of information within the other corporation therefore as a rule does not affect the secrecy management of the original holder undertaking.

- **Seeking an injunction or similar disposition against wrongful use by another corporation**

  When a corporation's trade secret is wrongfully used by another corporation, for the original holder undertaking to claim an injunction or similar disposition on the said other corporation requires that the holder undertaking's intent to manage its secrets be clearly indicated to the said other corporation (more specifically, the person responsible in the holder undertaking for sharing the said trade secret), just as it is indicated to your corporation's employees (this must be someone "to whom

[23] For example, cases such as developing AI (learning models) by using learning data for learning in the AI development and learning stage are assumed.
[24] However, if information α is provided not only to the company but also to a third party other than the company (e.g., a generative AI provider), secrecy management may be denied.

the trade secret holder has disclosed the trade secrets" as set forth in Article 2-1-7 of the Act).

*Note: In the cases where company E has shared a trade secret with company F (F manages the said trade secret as one of its own), whether the employee of F can be held responsible for leaking the trade secret is a matter of the existence or lack of recognizability on the part of the employees within F.

- More specifically, a typical case would be one in which the establishment of a non-disclosure agreement that identifies the trade secrets clarifies the holder undertaking's intent to manage its secrets. Besides that, it is theoretically possible to communicate a corporation's intent to manage its secrets as confidential in a written document or oral statement that stipulates that the corporation controls the relevant information as a trade secret. In terms of providing proof of the fact, however, it is desirable to create a document (for example, by indicating that fact in an invoice) instead of orally transmitting the corporation's intent to manage its secrets.

  *Note: The fact that a piece of information constitutes a trade secret does not mean that its use or other handling is subject to civil measures/criminal penalties. It is subject to civil measures/criminal penalties only when it is considered to be used for the "intent to obtain wrongful profits" or used for the "intent to cause damage to the holder", such as considerably violating the principle of good faith in light of the degree of confidence between the parties concerned, the benefits of each party concerned, the content of the trade secrets, and other issues.

- This applies when a company discloses the trade secrets to other corporations through joint research for example. An effective way for the holder undertaking to indicate its intent to manage its secrets would presumably be to establish a nondisclosure agreement involving the corporations and other stakeholders participating in the joint research and development to whom the trade secrets will be disclosed.

- On the other hand, even if for example, the holder shares a trade secret with another corporation without establishing a nondisclosure agreement that identifies the trade secrets, it does not in principle negate the secrecy management status relating to its own employees.

  *Note: However, should trade secret holder G have caused another corporation H to acquire and share its trade secrets without explicitly indicating its own intent to manage its secrets, despite there being no special reasons, and if some employees of corporation G understand that "although there were no special reasons, your

corporation G has caused H to acquire and share its trade secrets without explicitly indicating its intent to manage its secrets", then it is necessary to note that the recognizability of the employees of corporation G is weakened, and therefore the secrecy management status of G may be rejected.

3. Concept of usefulness

For "usefulness" to be recognized, the specific information should be objectively useful for business activities. Conversely, information of a nature which violates public welfare and morality including information on the antisocial conduct of a company cannot be recognized to be "useful".

(1) The "usefulness" requirement aims mainly to protect information recognized as commercially valuable in a broad sense, with information that produces little profit from being legally protected as a secret being excluded from the scope of trade secrets, such as information about criminal or other violations of public welfare and morality (information about tax evasion, careless release of harmful substances, and other antisocial conduct).

(2) Consequently, if the information is used/utilized in business activities of a business operator who possesses trade secrets, the necessity of protection as trade secrets can basically be recognized, and the requirement of usefulness is considered to be satisfied unless the information lacks the appropriateness of protection, such as the information violates public welfare and morality[25].
In addition, it does not need to be actually used in business activities.
It also includes information with indirect (potential) value. For example, research data about previous failures (the relevant information can be used to reduce research and development expenses), information about product defects (information that is important for the development of software based on artificial intelligence technology [26] that can be highly precise in detecting defective products), and other "negative" information, can also be recognized to be useful.

---

[25] See the decision by the Tokyo District Court, December 9, 2022; 2021 (Toku-Wa) 129, the decision by the Tokyo District Court, February 26, 2024; 2022 (Toku-Wa) 2148.
[26] Similarly to Contractual Guidelines concerning Artificial Intelligence and Data: Artificial Intelligence (June 2018) (hereafter, "The AI Guidelines") (https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20180615001-3.pdf), "AI technology" in the Guidelines refers to either machine learning or specific set of related software technology. The AI Guidelines define "machine learning" as "one learning method with which to discover specific rules from specific data, and estimate, predict, or intuit in order to compensate for inadequacies in a dataset, based on an understanding of those rules.

(3) When determining the usefulness requirement, it is not affected by whether a person who unlawfully obtained the information can effectively utilize it[27].

The usefulness quality of the information is not lost even if combining pieces of information available in the public domain can easily produce the relevant trade secret (this is unrelated to the concept of "progressiveness" in the patent system)[28].

A **typical court decision for reference**

・ "The purport of the protection of trade secrets under the Unfair Competition Prevention Act exists in protecting the advantageous competitive position that can be held based on information rightfully possessed in order to prevent unfair competition and maintain competitive order, but not in protecting progressive special information. Therefore, in order for such information to be considered useful technical information, it is not necessary for the information to produce "unexpected, particularly excellent effects." [Decision by the Yokohama District Court, July 7, 2021; 2018 (Wa) 1931, etc.].

4. Concept of not publicly known

For any information to be recognized as "not publicly known", it should be unknown to the public or difficult for the public to discover.

○ Status of "not publicly known"

・ The status of "not publicly known" means a state where the relevant trade secret is not generally known, or a state where it is not easily discovered[29]. Moreover, it refers to a state where the relevant information is not published in any publication that is available without a reasonable degree of effort, is not easy to estimate or analyze from published information, is not a generally available product, or something similar, or is in another similar state where no such information is generally available from any source other than the information under the control of the trade secret holder[30].

○ "A invention that is public knowledge" (Article 29-1-1 of the Patent Act)

・ The non-public domain requirement for trade secrets is not interpreted in the same way as "a invention that is public knowledge" (Article 29-1-1 of the Patent Act)

---

27 See the decision by the Tokyo District Court, December 9, 2022; 2021 (Toku-Wa) 129, the decision by the Tokyo District Court, February 26, 2024; 2022 (Toku-Wa) 2148.

28 See the decision by the Yokohama District Court, July 7, 2021; 2018 (Wa) 1931.

29 Article 39-2 (a) of the TRIPS sets forth similar requirements.

30 A state in which information is not known to the general public but can be easily learned cannot be considered non-public domain.

which is used in determining the novelty of a specific invention in the Patent Act. In the interpretation of the Patent Act, any information can be in the public domain if the relevant person has no obligation to keep it confidential even if only specific persons know the relevant information. In terms of trade secrets that are not publicly known, they may be considered not to be in the public domain if the information is only known by specific persons who keep it confidential. Moreover, if a third party other than the trade secret holder develops a similar trade secret of the same kind independently, and if the said third party keeps it as a secret, then it remains to be non-public domain.

○ "Previously published in a foreign publication"

・ Moreover, if the relevant information was actually published in a previous foreign publication, but the fact is unknown in the jurisdiction of the relevant information, and if it requires a considerable cost in terms of both time and capital to acquire it, then its being non-public domain can still be acknowledged. Naturally, if by investing such resources, a third party actually acquires or develops the relevant trade secret, subsequently publishing or similarly releasing it in the jurisdiction under question resulting in the information entering into a state of being "publicly known", then it no longer qualifies as "non-public domain".

○ If disclosed on the dark web

・ Even if trade secrets are disclosed on the dark web[31] due to hacking by a third party, etc., that alone does not immediately result in the loss of non-public domain.

○ Combination of information in the public domain

・ A "trade secret" usually consists of an item of information that is the result of combining know-how and other information. However, the fact that a fragment of information is published in various publications and that collecting those fragments could lead to a reconstruction of information similar to the information that constitutes the relevant trade secret does not immediately mean that the information is in the public domain. This is due to the fact that there can be several items of information or methodologies etc. that, if employed, would produce other outcomes, and if value lies in the question as to which items of information should be combined in what way, then those pieces of information can constitute a trade secret. Information is judged for applicability to the trade secret criteria by whether it can be generally obtained outside the control of the holder, and depending on its ease of combination, time and capital costs incurred in the process, or other efforts that are

[31] The term "dark web" as used herein refers to websites that cannot be accessed by ordinary means and cannot be found using search engines.

required for its acquisition[32]. For example, even if it is a combination of pieces of information in the public domain, if the combination is not known or not easily accessible, it can be considered non-public domain because it has not lost its financial value. Even if it is a combination of pieces of information in the public domain and the combination is known or easily accessible[33], if it has financial value due to the time and financial costs required to obtain it, it can be considered non-public domain.

○ Relationship with progressiveness (Article 29-2 of the Patent Act)

・ The purport of the protection of trade secrets under the Unfair Competition Prevention Act does not exist in protecting progressive special information; it therefore is not necessary for the information to produce "unexpected and particularly excellent effects" to be considered information in the non-public domain[34].

○ Reverse engineering

・ If trade secrets can be extracted by means of reverse engineering[35], the determination will differ depending on the degree of difficulty of extraction. Specifically, if trade secrets can be obtained by anyone by simply analyzing a product, it is considered to lose its non-public domain status because it is tantamount to disclosing the trade secrets themselves by placing the product on the market. On the other hand, if it requires special skills and a considerable amount of time to obtain and the trade secrets are not readily available to everyone, its non-public domain status will not be lost simply because the product has been placed on the market.

Typical court decisions for reference

An example of affirmation of trade secret status

・ In order to obtain the information through analysis of commercially available products, it is necessary to fully utilize the expertise of paint manufacturers and seek cooperation from raw material manufacturers, which requires a certain amount of time and is not readily available to everyone. For that reason, the court affirmed the claim that the relevant information was non-public domain [Decision by the Nagoya High Court, April 13, 2021; 2020 (U) 162].

[32] See the decision by the Nagoya District Court, March 18, 2022; 2017 (Wa) 427.

[33] Something such as data used for the development (learning) of AI technology created by combining information in the public domain is assumed.

[34] See the decision by the Tokyo High Court, February 17, 2022; 2021 (U) 1407.

[35] Reverse engineering as used here refers to the act of extracting information embodied in a product, such as its structure, materials, components, and manufacturing methods, by analyzing and evaluating the product, and using the extracted information.

An example of denial of trade secret status

- It is easy to determine the type of alloy and the mix ratio used in the plaintiff's product distributed on the market by using a commonly available technical method which is not excessively expensive. For that reason, the court denied the claim that the relevant information was non-public domain [Decision by the Osaka District Court, July 21, 2016; 2014 (wa) 11151; 2013 (wa) 13167]

Conclusion

Trade secrets are becoming increasingly important as a source of the competitiveness of Japanese companies.

On the other hand, their content and control methods are affected in complex ways by the nature of the information, the competitive environment with rival companies, the number of employees, the degree of global development in the field, the status of business consignment, and advances in telecommunications technology. The content and control methods of trade secrets are extremely diverse depending on the company, and incessant efforts will be required for managing them properly.

Companies are expected to operate in the spirit of these Guidelines, and utilize creativity toward the effective management of trade secrets suited to their respective circumstances.

Finally, we hope that all parties concerned will respect the creative management of trade secrets and that the parties will protect and utilize their trade secrets, thereby realizing a national system that will help revitalize the economic activity of Japan.

Management Guidelines for Trade Secrets

Issue date: January 30, 2003
Latest revision: March 31, 2025

Edited by: Intellectual Property Policy Office, Economic and Industrial Policy Bureau,
Ministry of Economy, Trade and Industry
1-3-1, Kasumigaseki, Chiyoda-ku, Tokyo 100-8901
Tel: +81-3-3501-1511 Extension: 2631
Email: bzl-chitekizaisan@meti.go.jp