VLT Legal Update

July 2025

Revisions to Trade Secret Management Guidelines

In March 2025, the Ministry of Economy, Trade and Industry ("***METI***") updated its Trade Secret Management Guidelines ("***Guidelines***") to reflect current changes in technology and recent legal trends. Some of the more salient revisions are described below, but the list is not exhaustive. Please contact us if you would like more information.

Definition of Trade Secret

In order for a "Trade Secret" to be protected under the Unfair Competition Prevention Act, a company needs to show that the information is technical or business information, which:

1. is **useful,**
2. **kept confidential** using appropriate control measures, and
3. is **not publicly known**.

Key Revision Provisions

Kept as Confidential Information

1. ***Appropriate Control Measures: Types of Parties***

   Previously the Guidelines did not distinguish between what constituted sufficient control measures depending on the party with access to the trade secrets. However, the recent amendments clarify what *may* be considered sufficient control measures based on the following types:

   a. **Employees and Directors:**
      i. What kind of system is in place in order for employees to be aware that the information is considered confidential and that special treatment is necessary.
   b. **Business Partners:**
      i. Whether confidential information was shared with a business partner after a confidentiality agreement was concluded.
      ii. The absence of a confidentiality agreement does not necessarily mean that there were insufficient control measures, and evidence of other measures may still be presented.

2. ***Appropriate Control Measures: Clarification of Measures for Employees and Directors***
   i. The recent amendments clarify that, if it is obvious to employees that the information is important and naturally expected to be treated as confidential information, the following general measures *may* be considered sufficient control measures based on the following types.
      a. IDs and passwords are used to restrict access when logging into company computers, etc.
      b. Work rules, confidentiality agreements, etc. include language prohibiting disclosure of confidential information.
   ii. Strictly limiting access on an employee-by-employee basis is not necessary, and broadly granting access rights to a specific department based on business necessity is considered to be sufficient limitations.

3. ***Appropriate Control Measures: Generative AI***

   With respect to Generative AI, if the following conditions exist:
   i. The information is kept and managed as a secret by one division of the company,

ii. The secret information is used learning data to train a model, and
iii. As a result of a prompt, the generative AI outputs information that contains the secret information and this generated output is made available to the same or a different division,

Then, these facts alone are not sufficient to show that the confidentiality of the information has been negated. **However, if the different division subsequently incorporates, distributes or otherwise provides the generated output containing the confidential information to an unspecified third party, the information would no longer be considered as "not publicly known".**

Not Publicly Known

Several issues with respect to whether information is considered to be known by the public have been discussed in recent years, and METI's perspective has been reflected in the Guidelines as follows:

1. **Information Leaked on the Dark Web**
   The mere fact that secret information has been published on the dark web does not mean that the information is no longer considered to be "non-public", and courts will still consider whether the information was generally known or easily accessible.
2. **Synthesizing Publicly Available Information**
   Even if the parts of the information are considered to be publicly known or easily accessible, if the combination of such publicly known or easily accessible information is not considered to be known or easily accessible (e.g. due to the time and cost needed to acquire the information), then such information would not be considered known or easily accessible, and the information would retain its proprietary value.
3. **Reverse Engineering**
   Whether or not the reverse engineering of a trade secret can be considered to have negated the non-public nature of the information depends on the level of difficulty for reverse engineering the information. In particular, if anyone can analyze the product and very easily reverse engineer the product, then the commercialization of the product is considered to be equivalent to disclosing the trade secret itself. However, if special skills are required and a considerable period of time is needed to reverse engineer the product, then merely making the product commercially available will not negate the non-public nature of the information.