Final Report on A Practical Guide to Safeguard Trade Secrets for MSMEs in APEC Economies

APEC Intellectual Property Rights Experts Group

June 2026

Asia-Pacific Economic Cooperation

Asia-Pacific
Economic Cooperation

Final Report on A Practical Guide to Safeguard Trade Secrets for MSMEs in APEC Economies

APEC Intellectual Property Rights Experts Group

June 2026

APEC Project: IPEG 102 2024A

Produced by
Korea Institute of Intellectual Property

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#226-CT-01.11

Table of Contents

1. Background

With the deepening interdependence of the global economy, needs to protect intangible assets from local or cross-border infringements are increasing. Especially, as innovative technologies have a crucial impact on a business's survival and growth, the importance of protecting trade secrets to prevent the leakage of core technologies has grown significantly.

Amid the increasing number of disputes over trade secrets, SMEs, lacking the specialized personnel, systems, and other resources to prevent technology leakage, face potential vulnerabilities to the misappropriation or leakage of their core technologies.

The need for effective trade secret management systems is underscored by findings from the 2022 Intellectual Property Protection Survey conducted by the Ministry of Intellectual Property (MOIP). The survey revealed that 51.2% of trade secret leaks were due to former employees, yet only 44.8% of companies implemented management practices such as conducting exit interviews and obtaining confidentiality agreements.[1] This indicates a significant gap in trade secret protection practices.

Although these survey results are specific to Republic of Korea, similar challenges are observed in other APEC economies, demonstrating the widespread need to establish robust management systems to protect trade secrets, particularly when employees leave a company.

While APEC economies have established frameworks for trade secret protection, there are variations in how these systems are implemented across different economies, leading to differences in the levels of protection, awareness, and utilization of existing protection mechanisms.

Against this background, the project aims to provide a practical guide for effective trade secret management and remedies against misappropriation, enabling SMEs to safeguard their competitiveness. By including best practices and case studies from various APEC economies, the practical guide and recommendations derived from the project will be particularly beneficial for SMEs engaged in regional business.

The project will also benefit all APEC economies by allowing them to consider more efficient frameworks or practices for safeguarding trade secrets in their businesses. The project will provide an opportunity for policymakers within APEC economies to establish and develop effective and harmonized frameworks for trade secret protection.

1 For more detailed information on the results of the 2022 Intellectual Property Protection Survey conducted by the Korean Intellectual Property Office (KIPO), please refer to the following KIPO website: https://kipo.go.kr/ko/kpoBultnDetail.do?menuCd=SCD0200618&ntatcSeq=19719&aprchId=BUT0000029&sysCd=SCD02#1 (last visit on 14 July 2025).

2. Objectives of the Project

The project aims to address significant challenges of protecting trade secrets for SMEs within APEC economies, focusing on their potential vulnerability to the misappropriation or leakage of trade secrets.

In that regard, the primary objective of the project is to improve the capacity of SMEs within APEC economies by developing and disseminating a practical guide to safeguard trade secrets for SMEs. The guidebook will help equip SMEs with strategies for managing their trade secrets and guidance on seeking remedies in case of infringement.

The secondary objective is to enhance the capacity of APEC policymakers in charge of intellectual property or industry policy by providing a broader view of IP protection mechanisms and a vital repository containing civil and criminal enforcement measures and cases across APEC. Together with the enhanced capacity and the powerful database, IP policymakers can develop robust policies and systems for protecting trade secrets of SMEs.

The purpose and primary objectives, as mentioned above, may be accomplished through step-by-step approaches as follows:

- Reviewing the current status of legislations, policies, and programs relevant to trade secret protection in APEC economies across different economic and industrial environments;
- Identifying the best practices for managing trade secrets within a business;
- Sharing and exchanging findings, knowledges and best practices among APEC economies; and
- Disseminating a practical guide to safeguard trade secrets to SMEs in APEC economies.

These approaches may be achieved as efficiently as possible through:

- A comprehensive preliminary investigation of literature and documents on the current status of legal frameworks and policies regarding trade secret protection in APEC economies;
- A survey with a questionnaire across APEC economies on the details of legislation, policies and other programs for trade secret protection, as well as on case studies or best practices related thereto;
- An in-depth comparative analysis of the current status of trade secret protection systems in the respective APEC economies, based on the results of the earlier investigation and survey; and
- A seminar or forum with experts and representatives from each APEC economy. This event will provide an opportunity for policymakers to share and exchange their opinions, experiences and knowledge in protecting trade secrets.

As a first step toward producing meaningful research outcomes on the protection of trade secrets for SMEs within the APEC region through the step-by-step implementation of the aforementioned tasks, this preliminary report has been prepared.

This preliminary report reviews the current status of legislations, policies, and systems related to trade secret protection in APEC economies with diverse economic and industrial environments, based on a comprehensive preliminary investigation of literature and documents concerning the legal frameworks and policies of APEC economies.

3. Legal Frameworks for Trade Secret Protection in APEC Economies

(1) Australia

1) Legal Framework

Australia does not have a standalone statute or regulatory framework governing trade secrets. Instead, trade secrets are protected under common law principles, particularly through contractual obligations such as confidentiality agreements. While Australia does not explicitly define "trade secrets" as a distinct legal term, the concept can be understood through the term "undisclosed information" as provided in the TRIPS Agreement, to which Australia is a signatory.

Although there is no specific legislation dedicated solely to trade secrets, various legal instruments impose confidentiality obligations to prevent the unauthorized disclosure of confidential information:

- *The Corporations Act 2001* prohibits company officers and employees from improperly using information obtained through their positions for personal gain or to harm the company. The duty of confidentiality continues even after the termination of employment.
- Trade secrets may also be protected through express or implied terms in contracts, including employment agreements and commercial contracts, which stipulate that disclosed information must be treated as confidential.
- *The Privacy Act 1988* empowers the Privacy Commissioner to consider the need to prevent the unfair disclosure of commercially sensitive information in its investigations and reports.
- *The Freedom of Information Act 1982* allows central agencies to refuse the disclosure of documents if doing so would result in a breach of confidence, thereby protecting trade secrets from competitors.

2) Civil Remedies

In Australia, civil actions can be initiated for trade secret misappropriation. Although there are no specific limitations for initiating a claim, if the misappropriation involves a breach of a confidentiality agreement, statutory limitation periods apply. In most jurisdictions, the limitation period is six years, while in the Northern Territory it is three years.

Damages awarded in trade secret litigation are generally based on equitable remedies. The principle of equitable compensation is to restore the injured party to the position they would have been in had the misappropriation not occurred. Punitive damages are not typically available except in cases involving copyright infringement or breach of contract. If the trade secret was protected under a contractual clause and the clause was breached, the plaintiff may claim punitive damages for the contractual breach.

3) Criminal Remedies

While trade secret misappropriation is primarily addressed through civil remedies, certain statutes provide for criminal penalties in specific circumstances. For instance, if a company officer or employee misuses confidential information obtained through their position for improper purposes, such as gaining a personal benefit or harming the company, they may be subject to criminal liability under Section 184 of *the Corporations Act 2001*.

Under this provision, it is a criminal offense for an individual to use information dishonestly:

- with the intention of gaining an advantage for themselves or someone else, or of causing detriment to the company; or
- recklessly, in a manner that could result in such advantage or detriment.

4) Economy-Specific Features

Because the protection of trade secrets in Australia is largely based on contract law and equitable duties, it is crucial to implement defensive mechanisms when entering into agreements. Key practices include:

- incorporating confidentiality clauses in employment and business contracts;
- using non-compete clauses to restrict former employees from engaging in competitive activities after termination; and
- applying exclusivity clauses in business arrangements to limit information sharing with third parties.

These contractual tools play a vital role in ensuring the enforceability of trade secret protections.

5) Cases and Precedents

Australian courts have clarified that in order to claim protection for confidential information, the information must be sufficiently identifiable and of a nature that qualifies as confidential.[2]

In Smith Kline and French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health, the court held that confidential information must be specifically identifiable and not merely described in general terms. It must also be demonstrable, and the quality of the information should be subject to assessment to determine its confidentiality. The defendant must be shown to have received and misused the information without the plaintiff's consent, either actually or through a threatened misuse.

2 For a more detailed explanation of the current state of trade secret protection in Australia, please refer to the following website: https://www.twobirds.com/en/insights/2020/australia/an-overview-and-update-on-the-protection-of-trade-secrets-in-australia (last visit on 14 July 2025).

(2) Brunei Darussalam

1) Legal Framework

Brunei Darussalam does not have specific legislation governing trade secrets. *The Official Secrets Act* exists, but it pertains to matters of public security and official secrecy, and does not extend to private sector trade secrets.[3]

Instead, trade secrets in Brunei Darussalam are protected under the common law doctrine of breach of confidence, inherited from the UK legal system. Consequently, UK case law serves as a persuasive authority in Brunei Darussalam courts when determining whether a breach has occurred.

To establish a breach of confidence, the following elements are considered:

(a) Whether the information or idea was confidential in nature from the outset;

(b) Whether an obligation of confidence arose, which may depend on whether a reasonable person in the recipient's position would have recognized the information as confidential;

(c) Whether the obligation was breached, typically through unauthorized disclosure or use.

Importantly, such claims can arise even in the absence of a contractual relationship, provided the recipient knew or ought reasonably to have known that the information was confidential and not to be disclosed.

Trade secrets may also be protected contractually, typically through employment contracts or non-disclosure agreements (NDAs). These contractual obligations may continue to apply after termination of employment. Therefore, when drafting contracts, parties should ensure that confidentiality provisions are clearly and properly incorporated to safeguard trade secrets.

2) Civil Remedies

There are no statutory civil remedies specific to trade secrets in Brunei Darussalam. However, if trade secrets are protected under a contractual relationship, a claim for breach of contract may be brought, and the injured party may seek damages for losses resulting from the breach.

In a breach of confidence claim, equitable remedies such as injunctions or account of profits may also be sought, though such claims remain grounded in common law rather than specific legislation.[4]

3) Criminal Remedies

As there is no statutory framework governing trade secrets, Brunei Darussalam does not provide for criminal sanctions in cases of trade secret misappropriation.

---

3 Please refer to the following website for the original text of Brunei Darussalam's *Official Secrets Act*: https://www.agc.gov.bn/AGC%20Images/LAWS/ACT_PDF/cap153.pdf (last visit on 10 July 2025).

4 For more detailed information on Brunei Darussalam's intellectual property system, please refer to the website of the International Trade Administration, United States Department of Commerce: https://www.stopfakes.gov/IPR-Toolkits (last visit on 14 July 2025).

4) Economy-Specific Characteristics

Brunei Darussalam lacks legislation specifically regulating trade secrets, such information can still be protected through contractual agreements. In practice, this places the burden on parties to proactively safeguard sensitive information by including well-drafted confidentiality clauses in employment or commercial agreements.

Ensuring that the terms clearly define what constitutes confidential or proprietary information is essential for enforceability and post-termination protection.

5) Cases and Precedents

There are currently no reported Brunei Darussalam court decisions involving trade secret misappropriation or breach of confidence. Since Brunei Darussalam adopts the UK common law system, case law from English courts is regarded as highly persuasive. Accordingly, in the event of similar disputes—such as those arising from employment contracts—legal proceedings in Brunei Darussalam would likely follow the principles established in UK jurisprudence.[5]

5 International Trade Administration, *supra note 4*.

(3) Canada

1) Legal Framework

Canada does not have a standalone statute dedicated to the protection of trade secrets. Instead, trade secrets are protected under general principles of civil law, including contract law and the duty of good faith. Business information that derives value from being kept confidential may qualify as a trade secret, and such information is typically safeguarded through a combination of people, systems, procedures, and contractual obligations.[6]

However, the definition of a trade secret is explicitly provided in the Criminal Code. Under Section 391(5) of the Criminal Code, a "trade secret" is defined as information that:

(a) is not generally known in the relevant trade or business;

(b) has economic value by virtue of not being generally known; and

(c) is the subject of reasonable efforts to maintain its secrecy.

This definition aligns with the internationally recognized three-pronged test for trade secrets—secrecy, commercial value, and reasonable efforts to maintain confidentiality—demonstrating that Canada's legal framework is consistent with global standards.

2) Civil Remedies

In Canada, civil remedies for trade secret misappropriation are grounded in common law principles. A trade secret owner may seek damages based on causes of action such as breach of contract, breach of fiduciary duty, unjust enrichment, or unlawful interference with contractual relations.

When evaluating whether the information in question constitutes a trade secret, whether the dispute involves misuse of the trade secret, and whether the trade secret owner is entitled to relief, courts generally consider the following factors:[7]

- the measures taken to maintain secrecy;
- the value of the information;
- the cost in money or time of creating or developing the information;
- the ease with which the information could be acquired or developed by others independently;
- the degree to which the owner regards and treats the information as confidential;
- the degree to which the recipient regards and treats the information as confidential;
- whether the recipient ought to have known that the information was confidential; and
- whether misuse of the information resulted in detriment to the owner.

6 For a more detailed explanation of Canada's trade secret protection system, please refer to the Canadian Intellectual Property Office website: https://ised-isde.canada.ca/site/canadian-intellectual-property-office/en/trade-secret-theft#Section1 (last visit on 14 July 2025).

7 *Ibid.*

3) Criminal Remedies

Section 391 of *the Criminal Code* (R.S.C., 1985, c. C-46) defines the term trade secret and criminalizes the improper acquisition of trade secrets. Under subsection 391(1), it is an offense to knowingly obtain a trade secret through deceit, falsehood, or other fraudulent means, or to communicate or make such a secret accessible to another person. This provision extends criminal liability beyond mere misappropriation to include the unauthorized disclosure or sharing of trade secrets with third parties.

Subsection 391(2) further criminalizes the acquisition or disclosure of a trade secret by a person who knows, or is wilfully blind to the fact, that the information was originally obtained through the commission of an offense. This reflects the legislative intent to deter not only the initial act of misappropriation but also the downstream circulation and use of unlawfully acquired trade secrets.

Subsection 391(3) stipulates that the offense may be prosecuted either by indictment, carrying a maximum penalty of up to 14 years' imprisonment, or by summary conviction in less serious cases. Subsection 391(4) provides a clear exception: criminal liability does not arise where the same information was acquired through reverse engineering or independent development.

Canada's *Criminal Code* thus establishes broad criminal liability not only for the primary misappropriation of trade secrets but also for their unauthorized dissemination and secondary use. These provisions reflect a robust commitment to the protection of confidential business information and the promotion of fair competition. In addition to serving corporate interests, this criminal regime plays a critical role in safeguarding technological and knowledge assets of the economy.

4) Economy-Specific Features

Canada does not have a dedicated federal statute governing trade secrets; instead, trade secret protection is generally derived from common law principles. The legal approach to trade secrets may vary slightly among provinces, but the overall framework remains consistent.

In Ontario, *the Employment Standards Act* (ESA)[8] explicitly prohibits non-compete agreements. A non-compete agreement is defined as a contractual provision that restricts an employee, after the termination of employment, from engaging in any business, occupation, or activity that competes with the employer. Under the ESA, employers are generally prohibited from entering into such agreements with employees, and any clause with similar effect is likewise deemed invalid. If an employer violates this provision, the clause is rendered void pursuant to the ESA's "automatic voiding" mechanism. (ESA §§ 67.1 and 67.2)

This restriction reflects a policy objective of safeguarding employee mobility and the freedom to choose one's occupation. It also suggests that trade secret protection should rely on other legal instruments such as non-disclosure agreements (NDAs) or implied duties of confidence, rather than non-compete clauses.

In most other provinces, trade secret protection is similarly grounded in common law doctrines such as breach of confidence or breach of contract, and the legal treatment does not vary significantly between jurisdictions.

8 The original text of *the Employment Standards Act* of Ontario, Canada, can be found on the following website: https://www.ontario.ca/laws/statute/00e41 (last visit on 14 July 2025).

5) Cases and Precedents

One of the most significant trade secret cases in Canada is *Cadbury Schweppes Inc. v. FBI Foods Ltd.*[9]

Cadbury Schweppes Inc. (hereinafter "Cadbury") manufactured and sold a mixed beverage under the "Clamato" brand. The company maintained secrecy over its product formulation, manufacturing process, and related business information. While Cadbury was headquartered in United States, its operations in Canada were conducted through its subsidiary, *Duffy-Mott Canada Ltd*.

At the time, Duffy-Mott subcontracted production of Clamato to Industrial Labelling Company, the predecessor to *FBI Foods Ltd*. (hereinafter "FBI"). Through this relationship, FBI gained access to Cadbury's product recipe and manufacturing information. After Duffy-Mott terminated the subcontract, FBI developed a competing product and launched it under the name "Caesar Cocktail," thereby entering into direct competition with Clamato. Cadbury brought legal action, claiming that FBI had misused its trade secrets and engaged in unfair competition.

The Supreme Court of Canada addressed three main issues:

(a) whether FBI's actions constituted a breach of a duty of confidence;

(b) whether the information in question met the legal threshold of a trade secret; and

(c) the appropriate scope of remedies for such misuse.

The Supreme Court held that FBI had breached its duty of confidence by using Cadbury's proprietary information without express authorization. However, it also recognized that FBI's product was not a wholesale replication of Cadbury's formula, but rather a combination of prior subcontract knowledge and general market expertise. Furthermore, the Court noted that Cadbury had not taken sufficient steps to maintain the secrecy of its information.

Ultimately, the Court found in favour of Cadbury on the grounds of breach of confidence, but declined to grant a full injunction or require disgorgement of profits. Instead, it awarded damages based on the harm suffered. This ruling is regarded as a foundational precedent in Canadian trade secret law, establishing key principles for determining what constitutes protectable confidential information and what remedies are appropriate for misuse.

Notably, the Court emphasized a fact-specific approach that considers the secrecy, commercial value, and protective efforts surrounding the information, rather than accepting a claim of confidentiality at face value. It also underscored the importance of proportional remedies that reflect the nature and extent of the misuse.

9 *Cadbury Schweppes Inc. v. FBI Foods Ltd.*, [1999] 1 S.C.R. 142 (28 January 1999). Refer to the following website for the Supreme Court of Canada's ruling on this case: https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1678/index.do (last visit on 14 July 2025).

(4) Chile

1) Legal Framework

In Chile, trade secrets are primarily governed by *the Law on Industrial Property (Ley de Propiedad Industrial)*[10] and *the Criminal Code*.

Chapter VIII of *the Industrial Property Law* specifically addresses trade secrets. According to Article 86, a trade secret refers to undisclosed information under the control of its holder that can be applied in productive, industrial, or commercial activities. For information to qualify as a trade secret, it must meet the following criteria:

(a) it must be secret,

(b) it must have commercial value due to its secrecy, and

(c) it must be subject to reasonable measures to preserve its confidentiality.

These conditions align with the internationally recognized three elements of trade secret protection.

Article 87 defines acts of trade secret misappropriation. These include unauthorized acquisition, disclosure, or use of the information, as well as breach of confidentiality obligations by individuals with lawful access. Such acts constitute misappropriation when carried out for the benefit of oneself or a third party, or with the intent to cause harm to the trade secret holder. Chilean law places emphasis on intent, and when intentional misappropriation is established, strong legal liability may be imposed.

For information to be protected as a trade secret, it must not be generally known or readily accessible—whether in whole or in the specific arrangement of its components—by individuals within the relevant circles who routinely deal with such information. This implies that the information must be sufficiently specific and non-obvious to experts in the field. Non-public disclosure and access control are essential; for instance, a company may limit access to only certain employees and implement confidentiality agreements to protect the information.[11]

2) Civil Remedies

Pursuant to Article 88 of *the Industrial Property Law*, any misappropriation of trade secrets is subject to the enforcement provisions set out in Title X of the same law.

When industrial property rights are infringed or affected, the right holder may request various remedies including:[12]

10 Law No.19.039 of March 6, 2006, on Industrial Property (Consolidated Law approved by Decree-Law No.4 of 30 June 2022, incorporating amendments up to Law No. 21.355 of 5 July 2021).

11 For a more detailed explanation of Chile's trade secret protection, please refer to the following website: https://alessandri.legal/en/trade-secrets-and-current-trends-in-chile/ (last visit on 14 July 2025).

12 Chile's *Industrial Property Law*, Article 106.

- injunctive relief to cease the infringement;
- monetary damages;
- adoption of necessary measures to prevent further infringement; and
- publication of the court's ruling at the infringer's expense through media of the claimant's choice.

Damages may be assessed in accordance with general legal principles, or, at the claimant's election, based on one of the following measures:[13]

- the profits the claimant would have obtained if the infringement had not occurred;
- the gains acquired by the infringer as a result of the infringement; or
- a reasonable royalty that the infringer would have paid under a licensing agreement.

A person who sells products that infringe an industrial property right shall not be held liable for damages if they were unaware of the infringing nature of the goods at the time of the sale.[14]

3) Criminal Remedies

Pursuant to Article 88 of *the Industrial Property Law*, criminal liability may be imposed in addition to civil remedies in cases of trade secret misappropriation. In 2021, Chile enacted *the Law on Economic Crimes (Ley de Delitos Económicos)*, which introduced six new provisions explicitly addressing the criminal consequences of trade secret infringement, thereby reinforcing the legal framework in connection with *the Industrial Property Law*.

Article 284 of *the amended Criminal Code* prohibits unauthorized access to and reproduction of trade secrets. Accessing or reproducing a trade secret without the consent of the rightful holder constitutes a criminal offense, particularly when such acts are committed with the intent to disclose the secret or to obtain an economic advantage. In such cases, the penalty may include imprisonment corresponding to the medium level of presidio menor (presidio menor en su grado medio), as defined under the applicable criminal sentencing framework:

- Physical intrusion or eavesdropping : the act of visually or acoustically intruding, using technical devices, into company premises designed to be imperceptible from the outside;
- Recording private conduct or conversations: visually filming or aurally intercepting behaviour or speech occurring in situations where the individuals have a reasonable expectation of privacy;
- Unauthorized or excessive access: bypassing technical or security systems to infiltrate restricted information networks.

Reproducing trade secrets obtained through such means is also punishable. Furthermore, where the misappropriated trade secret is either disclosed to third parties or made accessible to them, enhanced penalties — including a higher degree of imprisonment — may apply.

13 Chile's *Industrial Property Law*, Article 107.

14 Chile's *Industrial Property Law*, Article 108.

Article 284bis establishes criminal liability for the unauthorized disclosure of trade secrets obtained through a relationship of trust. This includes violations by public officials or licensed professionals who breach confidentiality obligations arising from law or professional ethics, as well as individuals who disclose information acquired through employment or contractual relationships. In such cases, the penalty consists of imprisonment corresponding to the medium level of presidio menor (presidio menor en su grado medio), as defined under the applicable sentencing framework.

Article 284ter penalizes the unlawful use of trade secrets. Individuals who knowingly use trade secrets obtained through improper means for economic gain are subject to criminal sanctions. This applies even if the information was obtained indirectly, provided the user was aware of its illicit origin.

Article 284quater imposes professional disqualification when the offender is a member of a regulated profession. If the trade secret infringement occurs in the course of performing professional duties, the court may impose, in addition to imprisonment, suspension or revocation of the offender's license or qualifications. This reflects the seriousness of breaching public trust and professional ethics.

Article 284quinquies establishes a limitation on the scope of criminal liability, clarifying that the use of general knowledge, skills, or experience legitimately acquired through one's profession or previous employment does not constitute a criminal offense. This provision seeks to draw a clear distinction between trade secrets and general industry know-how, thereby safeguarding the right to pursue one's lawful occupation and ensuring the legitimate transfer and use of non-confidential technical knowledge.

4) Economy-Specific Features

According to guidance published by the Latin America IP SME Helpdesk, several best practices are recommended to ensure the protection of trade secrets under Chilean law:[15]

- Include confidentiality clauses in employment contracts. The Chilean Ministry of Labour acknowledges that confidentiality obligations may extend beyond the termination of employment.
- Mark documents containing trade secrets with labels such as "confidential" or "do not reproduce" to signal their sensitive nature.
- Execute non-disclosure agreements (NDAs) with industry partners who receive confidential information, and include contractual remedies such as damages for breach of confidentiality.
- Assess alternative legal protection tools. It is important to define which portions of information qualify as trade secrets and which are protected under registered intellectual property rights.
- Establish internal systems for trade secret protection, including company-wide policies and training. Clear procedures should be defined for managing, protecting, labelling, distributing, and eventually disclosing trade secrets.
- Prioritize and classify trade secrets based on their strategic importance to the business.
- Restrict access to trade secrets to a limited group of individuals, and ensure that all relevant parties are aware of the confidential nature of the information and the potential consequences of unauthorized disclosure.
- Implement robust cybersecurity systems to limit access to digital trade secrets. This includes monitoring and tracking access to sensitive data in order to prevent and detect unauthorized use.

15 Latin America IP SME Helpdesk, 'Trade Secrets in Chile: A guide for EU SMEs', European Commission (2021). For the original text of the report by the Latin America IP SME Helpdesk, please refer to the following website: https://www.cde.ual.es/wp-content/uploads/2021/09/EA0320482ENN.en_.pdf (last visit on 14 July 2025).

- Limit access to physical devices or hardware that store or process trade secret information.

These measures are not legally mandated but are highly recommended as evidence of reasonable steps taken to maintain secrecy—one of the essential legal conditions for qualifying information as a trade secret under Chilean law.

5) Cases and Precedents

As of the time of writing, no publicly available court decisions have been identified in Chile that specifically involve trade secret misappropriation or contractual breaches concerning trade secrets.

(5) People's Republic of China

1) Legal Framework

Trade secrets in People's Republic of China are primarily governed by the *Anti-Unfair Competition Law of People's Republic of China (AUCL)*, as revised on 27 June 2025 and effective as of 15 October 2025. The AUCL is supplemented by relevant provisions of the Civil Code, Criminal Law, Labour Contract Law, Company Law, and the Law on the Promotion of the Transformation of Scientific and Technological Achievements, as well as judicial interpretations, in particular the Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases Involving Infringement of Trade Secrets (effective 12 September 2020, currently valid).

Pursuant to Article 10 of the AUCL, business operators shall not commit the following acts of infringing on trade secrets:

- Acquisition of trade secrets through improper means such as theft, bribery, fraud, coercion, electronic intrusion, or other improper means;
- Disclosure or use of trade secrets obtained through improper means, or allowing others to use such trade secrets;
- Disclosure or use of trade secrets in violation of confidentiality obligations or the right holder's requirements for keeping the trade secrets confidential;
- Inducing, instigating, or assisting a third party to breach confidentiality obligations or confidentiality requirements in order to obtain, disclose, use, or allow others to use trade secrets.

Expanded Liability:

- Natural persons, legal persons, and unincorporated organizations other than business operators that commit the illegal acts listed above shall be deemed to have infringed on trade secrets.
- A third party that, with knowledge or should have known that an employee or former employee of the right holder or any other entity or individual has committed the illegal acts, still obtains, discloses, or uses such secrets shall also be deemed to have infringed on trade secrets.

Definition of Trade Secrets:

- For the purposes of this Law, trade secrets mean technical information, operational information and other commercial information that is not known to the general public, has commercial value and for which the right holder has taken corresponding confidentiality measures.

2) Civil Remedies

Civil remedies for trade secret misappropriation include injunctive relief and monetary compensation. In accordance with the principle that "the burden of proof lies with the party asserting the claim", prior to initiating litigation, plaintiffs are generally required to submit evidence proving that they have adopted confidentiality measures for the trade secrets claimed and reasonably indicating that the trade secrets have been infringed by the defendant.

In accordance with **Article 39 of the Anti-Unfair Competition Law**, the allocation of the burden of proof in trade secret infringement cases is structured as follows:

- Where the claimant provides preliminary evidence demonstrating that it has taken confidentiality measures with respect to the claimed trade secrets and reasonably indicates that the trade secrets have been infringed, the defendant shall bear the burden of proving that the information claimed by the right holder does not constitute trade secrets.
- Where the claimant provides preliminary evidence reasonably indicating infringement and further provides any of the following evidence, the defendant shall bear the burden of proving that it has not infringed the trade secrets: (i) evidence that the defendant had access to or an opportunity to obtain the trade secrets and that the information it used is substantially identical to the trade secrets; (ii) evidence that the trade secrets have been disclosed, used, or face a risk of disclosure or use; or (iii) other evidence that the trade secrets have been infringed.

The statute of limitations for civil claims begins when the right holder becomes aware, or should have become aware, that the right has been infringed and of the person who owes the obligation. The general limitation period is three years. Where more than 20 years have elapsed since the infringement occurred, the People's Court will no longer protect the relevant civil rights. Under special circumstances, the People's Court may decide to extend the limitation period upon application by the right holder.

Damages are calculated based on the losses suffered by the right holder or the benefits obtained by the infringer, as follows:

- Where actual losses can be determined, damages are calculated based on the losses suffered by the right holder as a result of the infringement.
- Where actual losses are difficult to determine, damages may be calculated based on the benefits obtained by the infringer from the infringement.
- Where the right holder requests that damages be determined by reference to a licensing fee for the trade secret, the People's Court may determine the amount by taking into account factors such as the nature and content of the license, its actual performance, and the nature, circumstances, and consequences of the infringement.
- Reasonable expenses incurred by the right holder to stop the infringement may also be supported in accordance with the law.

3) Criminal Remedies

Article 219 and Article 219-1 of the Criminal Law of People's Republic of China stipulate crimes involving trade secrets, among which Article 219 prescribes the criminal liabilities for the crime of infringing on trade secrets, and Article 219-1 prescribes the criminal liabilities for the crime of stealing, spying, buying, or illegally providing trade secrets for parties outside the territory of People's Republic of China.

Offenses constituting the crime of infringing trade secrets (Article 219) include:

- Obtaining a right holder's trade secrets by theft, bribery, fraud, coercion, electronic intrusion, or any other improper means;
- Disclosing, using, or allowing others to use trade secrets obtained by the means specified above;
- Disclosing, using, or allowing others to use trade secrets in violation of confidentiality obligations or the right holder's requirements for keeping the trade secrets confidential;

Knowingly obtaining, disclosing, using, or allowing others to use trade secrets as described above shall be deemed to have infringed on trade secrets.

Penalties for Article 219:

- Anyone who commits any of the above acts and the circumstances are serious shall be sentenced to fixed-term imprisonment of not more than three years and shall also, or shall only, be fined;
- If the circumstances are especially serious, the offender shall be sentenced to fixed-term imprisonment of not less than three years but not more than ten years and shall also be fined.

Penalties for Foreign-Related Misappropriation (Article 219-1)

- Whoever steals, spies, buys or illegally provides trade secrets for entities, organizations, or individuals outside the territory of People's Republic of China shall be sentenced to fixed-term imprisonment of not more than five years and shall also, or shall only, be fined;
- If the circumstances are serious, the offender shall be sentenced to fixed-term imprisonment of not less than five years and shall also be fined.

Even where trade secret infringement is established in a civil proceeding, this does not automatically result in a criminal conviction. First, acts of infringing trade secrets constitute a crime only where the statutory requirement of "serious circumstances" is satisfied. Second, civil cases are adjudicated based on a high probability standard, whereas criminal convictions require that the facts are clear, the evidence is reliable and sufficient, and that guilt is established beyond a reasonable doubt. Accordingly, the evidentiary threshold for criminal proceedings is significantly higher than that applied in civil litigation.

4) Economy-Specific Features

The severity of criminal punishment varies depending on the criminal circumstances of the infringement. In accordance with relevant judicial interpretations, acts of infringing trade secrets shall be deemed to constitute "serious circumstances" as stipulated in Article 219 of the Criminal Law where any of the following conditions are met:

- Losses caused to the right holder of the trade secrets amount to more than CNY 300,000 (approximately USD 42,000);
- Illegal gains obtained from infringing trade secrets amount to more than CNY 300,000;
- Losses or illegal gains amount to more than CNY 100,000 where the offender has, within the preceding two years, received criminal punishment or administrative penalties for acts stipulated in Article 219 or Article 219-1 of the Criminal Law; or
- Other circumstances that are deemed serious.

Acts of infringing trade secrets shall be deemed to constitute "especially serious circumstances" where:

- The infringement directly causes the right holder of the trade secrets to go bankrupt or to shut down due to major operational difficulties; or
- The amount of losses or illegal gains reaches ten times the corresponding thresholds set forth for serious circumstances.

Model trade secret protection practices encouraged under relevant judicial interpretations include:

- Requiring confidentiality agreements or including confidentiality clauses in employment contracts;
- Providing confidentiality instructions to employees, suppliers, customers, and visitors through internal rules, guidelines, or written notices;
- Restricting access to production and business areas where trade secrets are present;

- Labelling, classifying, isolating, encrypting, or sealing trade secrets and limiting access exclusively to authorized personnel;
- Imposing restrictions on the use, access, and duplication of computer, electronic, and network equipment used to store or transmit trade secrets;
- Requiring departing employees to return, delete, or destroy confidential materials and to reaffirm their continuing confidentiality obligations.

However, the specific application of these practices may vary depending on the technical field. For example, in areas such as software development, it is often recommended to divide development tasks into separate modules handled by different personnel in order to limit access to complete technical information.

5) Cases and Precedents

Courts allow for the application of punitive damages in trade secret cases involving willful or malicious infringement, permitting awards of one to five times the amount of the actual losses suffered by the right holder or the unlawful gains obtained by the infringer.

In 2024, the Supreme People's Court adjudicated a trade secret infringement case involving nearly 40 former senior managers and technical personnel who successively left their positions. The disclosure, use, and authorization for others to use the technical secrets at issue were found to constitute trade secret infringement. Taking into account the unlawful gains derived from the infringement, the court ordered the defendant to pay compensation of approximately CNY 638 million (around USD 90 million).[16]

According to publicly available information released by the State Administration for Market Regulation (SAMR), as of June 2025, market regulation authorities handled 14,188 unfair competition cases in 2024, including 143 cases involving trade secret infringement.[17] Representative enforcement scenarios include:

- Unauthorized acquisition of product drawings using a mobile phone by an employee during active employment, despite the existence of confidentiality and computer usage agreements;
- Transfer of project-related data to personal email accounts by a departing engineer during the handover process;
- Disclosure of confidential documents via social media or messaging applications in violation of non-disclosure agreements;
- Post-employment development of products found to be substantially identical to a former employer's trade secrets;
- Unauthorized access to enterprise information systems, such as ERP systems, by using another employee's credentials to obtain confidential pricing or sales data.

16 For more detailed information on this case, please refer to the website of the Intellectual Property Court of the Supreme People's Court of China: https://ipc.court.gov.cn/zh-cn/news/view-3092.html (last visit on 10 July 2025).

17 For more detailed information on trade secret infringement cases in China, please refer to the following website: https://credit.cngy.gov.cn/detail.do?contentId=d4288d717a0241e79deaabb224c3c018&channelId=60a1ca1108aa43af9d48c526404268db (last visit on 10 July 2025).

(6) Hong Kong, China

1) Legal Framework

Trade secrets and its equivalent may, depending on the circumstance, cover a variety of confidential information which may be technical (e.g. formulas, food/drink recipes, know-how, manufacturing methods, designs, product specifications etc.) or commercial (e.g. supplier/client lists with commercial value the compilation of which involves mental processes, judgment, labour and skills, business strategies and methods etc.) in nature.

As a common law jurisdiction, Hong Kong, China protects trade secrets and its equivalent by the law of confidence under common law. It does not have a specific trade secret legislation.

As distilled from case law authorities, a trade secret or its equivalent refers to information which—

(a) is used in a trade or business;

(b) is confidential, i.e. not already in the public domain;

(c) can be easily isolated from other information which the employee is free to use so that any man of average intelligence and honesty would think it is improper to use the information at the disposal of his new employer;

(d) (if disclosed to a competitor) would be liable to cause real or significant harm to the owner of the information; and

(e) the owner must limit its dissemination or at least not encourage or permit its widespread publication or otherwise impress upon the employee the confidentiality of the information.[18]

Expressed or implied terms of binding contracts, trade customs or industry practices may also give rise to an obligation of confidence.

To enhance legal protection of confidential information, it is strongly recommended that Non-Disclosure Agreements (NDAs) be executed as far as practicable between the owner of the information and an individual to whom the information is to be imparted or who may be exposed to such information.

2) Civil Remedies

Owners of trade secrets may institute civil proceedings against breach of confidence for remedies, including injunctions, damages/account of profits damages/account of profits, delivery up of materials containing the confidential information.

Injunctions are generally granted where monetary damages are considered an inadequate remedy. In appropriate cases, a plaintiff may seek an interim injunction to prevent the defendant from disposing of assets or attempting to do so. Such relief may also be granted to restrict the use of disputed information, particularly where there is a risk of irreparable harm or dissipation before the case is adjudicated.

18 *AXA China Region Insurance Company Limited v Pacific Century Insurance Company Limited and others* [2003] 3 HKC 1

3) Criminal Remedies

Hong Kong, China does not have a specific criminal offence targeting misappropriation or misuse of trade secrets on its own. Where the overall circumstance and evidence of an individual case involving such misappropriation or misuse also contain the requisite elements of an applicable offence (e.g. where the wrongful conduct in question also involves fraud, deception or otherwise dishonesty punishable by the criminal law), the case may be caught by the criminal net which however has to be determined on a case-specific basis.

4) Economy-Specific Features

While trade secrets may be protected under common law, there may exist individual circumstances where the public interest in disclosure of confidential information outweighs maintaining its confidentiality, particularly where the information in question pertains to serious wrongdoing (notably criminal offence), public health or safety, under which the informer in question may be protected from liability in accordance with the applicable law even though his/her obligation on confidence is technically breached.

Some illustrations of lawful disclosure

- An employer may not dismiss an employee for giving evidence in any proceeding or inquiry for the purposes of the enforcement of the *Employment Ordinance* (e.g. proceedings relating to workplace safety).[19]

- A person who discloses information relating to drug trafficking, money laundering, or criminal proceeds is not considered to be in breach of confidentiality clauses under contracts, statutes, or codes of conduct. Such person is also shielded from liability for any damages resulting from the disclosure.[20]

5) Cases and Precedents

- ***AXA China Region Insurance Company Limited and another v Pacific Century Insurance Company Limited and others [2003] 3 HKC 1***

The plaintiffs were AXA group of insurance companies ("AXA"). The 1st defendant ("PCI") was a competing insurance company and the other defendants were former AXA insurance agents who had subsequently joined PCI. AXA found that client data (including personal particulars of policyholders as well as details of the sold policies) stored in their computer system (to which access is restricted) have been misappropriated by the individual defendants during their agency with AXA. At about the same time, PCI launched a policy matching scheme to lure AXA clients to surrender their AXA policies and switch to PCI policies. AXA took legal action against PCI and the individual defendants for wrongfully obtaining confidential information belonging to AXA and for breach of confidence.

19 *Employment Ordinance* (Cap. 57) of Hong Kong, China, Section 72B.

20 *Drug Trafficking (Recovery of Proceeds) Ordinance (DTRPO)* (Cap. 405) of Hong Kong, China, Section 25A(3); *Organized and Serious Crimes Ordinance (OSCO)* (Cap. 455) of Hong Kong, China, Section 25A(3); *United Nations (Anti-Terrorism Measures) Ordinance (UNATMO)* (Cap. 575) of Hong Kong, China, Section 12(3).

The court held that the client data in question qualified as protectable trade secret under the five-step test (see the 3rd paragraph under "Legal Framework" above) derived from well-considered authorities, and granted the injunction sought against both PCI and the individual defendants.

- ***Conpak Management Consultants Limited v. Luk Wai Ting [2024] HKDC 1545***

The District Court of Hong Kong, China rejected Conpak's application for an injunction against a former employee, Luk Wai Ting. While employed at Conpak, Luk transferred 223 emails from his work email to his personal account. After moving to a competing firm, he contacted former clients of Conpak using his new work email, offering discounted services and referencing his previous employment.

Conpak argued that client contact information constituted confidential information. However, the court found no evidence to support that claim. The identities of the clients mentioned in the emails were not disclosed in court, and no content from the emails was presented to substantiate the claim of confidentiality.

Accordingly, the court ruled that there had been no breach of confidence and dismissed the injunction application.

This case highlights the importance of clearly identifying and substantiating confidential information before initiating legal proceedings. Employers should assess whether the information they seek to protect satisfies the legal criteria for confidentiality.[21]

21 Simmons & Simmons, 'Hong Kong Court: Client Contacts Not Confidential in Conpak v Luk', Simmons & Simmons (25 October 2024), For the original text of this article, please refer to the following website: https://www.simmons-simmons.com/en/publications/cm2myu60h0050tqmoirzgodn7/hong-kong-court-client-contacts-not-confidential-in-conpak-v-luk (last visit on 10 July 2025).

(7) Indonesia

1) Legal Framework

Trade secrets in Indonesia are governed by *Law No.30 of 2000 concerning Trade Secrets (TSL)*.[22] According to Article 1(1), a trade secret is defined as information that is not generally known to the public in the field of technology and/or business, has economic value due to its usefulness in business activities, and is maintained as confidential by its owner.

Trade secrets may include methods of production, processing, sales strategies, or other information related to technology or business that:[23]

- Is not publicly known;
- Is economically value;
- Is subject to reasonable efforts to maintain confidentiality.

If information is known only to a limited group or not accessible to the general public, and if it is used for commercial operations or economic advantage, it is deemed to have economic value. The confidentiality requirement is satisfied where the owner or controller of the information takes adequate and appropriate measures to maintain its secrecy.[24]

The owner of a trade secret has the right to use the secret personally, or to authorize or prohibit others from using or disclosing the trade secret to third parties for commercial purposes.[25]

Misappropriation arises when a trade secret is disclosed intentionally, in breach of a confidentiality obligation—whether contractual, written, or implied—or acquired or possessed in violation of law or regulation.[26] However, use or disclosure is not considered misappropriation where it serves the interests of public security, public health, or safety, or when reverse engineering is conducted solely for further product development.[27]

2) Civil Remedies

The owner or licensee of a trade secret may initiate legal proceedings for damages and injunctive relief against any person who has wilfully misappropriated the trade secret without authorization.[28] Indonesia notably allows licensees to bring trade secret claims, distinguishing its approach from some jurisdictions where only the owner has standing.

---

22 Law of the Republic of Indonesia Number 30 Year 2000 Regarding Trade Secret (20 December 2000). For the original text of Indonesia's legislation regarding trade secrets, please refer to the following website: https://wipolex-resources-eu-central-1-358922420655.s3.amazonaws.com/edocs/lexdocs/laws/en/id/id041en_1.pdf (last visit on 14 July 2025).

23 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 2.

24 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 3.

25 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 4.

26 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 13 and 14.

27 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 15.

28 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 11.

3) Criminal Remedies

Any person who wilfully misappropriates a trade secret without authorization may face up to two years' imprisonment or a fine of up to IDR 300 million. Trade secret infringement constitutes a complaint-based offense requiring the right holder's formal complaint for prosecution.[29]

4) Economy-Specific Features

The Trade Secret Law provides for the assignment and licensing of trade secret rights, which must follow formal procedures. Trade secrets may be transferred by inheritance, gift, testament, written agreement, or other legal means, but such transfers must be registered with the Directorate General of Intellectual Property (DGIP). An unregistered transfer has no legal effect against third parties.[30]

Similarly, trade secret licenses must be registered with the DGIP to be legally effective vis-à-vis third parties. Licensing agreements must not contain clauses that could harm the Indonesian economy or violate competition laws.[31] All assignments and licenses must be published in the Official Gazette.[32]

In addition, Indonesia empowers designated IP enforcement officials to investigate criminal acts related to trade secrets, in parallel with the regular police force. These officials may conduct:[33]

- Investigations into the veracity of complaints or reports;
- Interviews and information gathering from relevant parties;
- Collection of evidence and documents;
- Inspections of materials related to the offense.

5) Cases and Precedents

While a legal framework for trade secret protection exists, its effectiveness may be limited by insufficient judicial awareness or interpretive capacity.

In a notable case, PT Basuki, a European engineering company, filed a lawsuit against a major Indonesian construction firm and associated parties, alleging misappropriation of proprietary boiler design know-how. The plaintiff claimed that confidential technical data had been unlawfully used to develop a competing product.

However, the Bekasi District Court dismissed the case, reasoning that the dispute fell within the jurisdiction of the Commercial Court, citing precedent from an earlier industrial design case between the same parties. On appeal, the Supreme Court of Indonesia reversed this decision, holding that trade secret cases fall under district court jurisdiction, and that the lower court had misapplied the law.

---

29 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 17.

30 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 5.

31 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 6 and 7.

32 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 5 and 6.

33 Indonesia's *Law No.30 of 2000 concerning Trade Secrets*, Article 7.

The case was remanded and is currently being reheard in the district court. This incident reflects a broader challenge seen across developing Southeast Asian IP systems—the presence of legal instruments but inconsistent judicial application, often due to limited training or experience with trade secret disputes.[34]

34 South-East Asia IP SME Helpdesk, 'Case Study 01 – Inexperience of Indonesian courts with trade secret cases', European Commission. For the original text of the report by the South-East Asia IP SME Helpdesk, please refer to the following website: https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/south-east-asia-ip-sme-helpdesk/case-studies/case-study-01-inexperience-indonesian-courts-trade-secret-cases_en (last visit on 14 July 2025).

(8) Japan

1) Legal Framework

In Japan, trade secrets are primarily governed by *the Unfair Competition Prevention Act (UCPA)*, supplemented by general provisions of *the Civil Code* related to torts, unjust enrichment, and contract law. Under Article 2 of the UCPA, a trade secret is defined as technical or business information useful for business activities, that is kept secret, and not publicly known.

Trade secret misappropriation is considered a type of unfair competition under the UCPA. Specific acts constituting misappropriation include:

- Acquiring trade secrets by theft, fraud, duress, or other wrongful means;
- Using or disclosing trade secrets acquired through an act of wrongful acquisition;
- Acquiring, using, or disclosing trade secrets while knowing there has been a wrongful acquisition, or while not knowing this fact due to gross negligence
- Using or disclosing trade secrets, after acquiring those trade secrets and learning that there had been an act of wrongful acquisition, or while not knowing this fact due to gross negligence (there are some exceptions);
- Using or disclosing trade secrets provided by a trade secret holder for the purpose of wrongful gain or to cause damage to the trade secret holder;
- Acquiring trade secrets while knowing that the disclosure of trade secrets constitutes improper disclosure, or knowing that there has been improper disclosure of the relevant trade secrets, or while not knowing this fact due to gross negligence;
- Using or disclosing trade secrets acquired in such a manner;
- Using or disclosing trade secrets, after acquiring those trade secrets and learning that the relevant acquisition constitutes an act of improper disclosure of trade secrets, or that there had been an act of improper disclosure with regard to the relevant trade secrets, or while not knowing this fact due to gross negligence (there are some exceptions);
- Transferring, delivering, displaying for the purpose of transfer or delivery, exporting, importing, or providing through telecommunications lines things created by any of the acts stated above (those acts being limited to acts of using a technical secret) (there are some exceptions).

2) Civil Remedies

Claims for damages resulting from trade secret infringement are subject to the general statute of limitations for torts. The right to claim extinguishes either three years after the victim or their legal representative comes to know the damage and the identity of the perpetrator, or twenty years from the time of the tort, whichever is earlier.

Regarding the calculation of damages, there are the following estimation provisions:

- The profit the trade secrets owner would have earned but for the infringement (i.e., the amount of profit per unit of the infringed party's things or service multiplied by the quantity of the things or service that infringer transferred or provided);
- The profits made by an infringer through the act of infringement;

- Equivalent to the royalties

The infringer may overturn this presumption by proving that such profits were derived from factors unrelated to the infringed trade secret, such as brand value or marketing activities. In Japan, punitive damages are not recognized in the first place, and punitive damages for trade secret infringement are also not recognized.

3) Criminal Remedies

Acts such as acquiring trade secrets through theft, unauthorized access, or fraud, as well as unauthorized use or disclosure by insiders, including after resignation, may be subject to criminal penalties.

If the trade secret is misappropriated for use outside Japan or actually used outside Japan, aggravated penalties may apply. Attempted offenses are also punishable, and proceeds derived from the offense may be confiscated. Foreign residents may also be subject to punishment if they infringe on the trade secrets of Japanese entities.

4) Economy-Specific Features

Japan recognizes a separate category of information known as "shared data with limited access", which refers to technical or business information that is accumulated to a significant extent and managed by electronic or magnetic means, and is intended to be provided to specific persons on a regular basis. To qualify as shared data with limited access, the information must meet the following requirements:

- Provided to specific persons on a regular basis;
- Accumulated to a significant extent by electronic or magnetic means; and
- Managed by electronic or magnetic means.

The key difference is that shared data with limited access may not be strictly confidential, whereas trade secrets must be non-public and must be kept secret. Moreover, shared data with limited access must be in electronic or magnetic form, while trade secrets may exist in any format. However, unfair competition acts related to shared data with limited access is not subject to criminal penalties.

In March 2025, Japan issued a revised version of the Management Guidelines for Trade Secret in response to changes in the working environments, changes in information management methods, etc.[35] The updated guidelines have clarified the requirements for protection as trade secrets, taking into account the changes in circumstances described above.

5) Cases and Precedents

In Japanese trade secret litigation, whether information constitutes trade secrets may be an issue of dispute. In order to be recognized as trade secrets, the following three requirements must be met:

(a) Secrecy management (the information must be kept secret),

(b) Usefulness (it must be useful technical or business information), and

35 Ministry of Economy, Trade and Industry (METI) of Japan, 'Management Guidelines for Trade Secret', METI (2025). For original text of the Management Guidelines for Trade Secret published by the Ministry of Economy, Trade and Industry (METI) of Japan in January 2003, please refer to the following website: https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf (last visit on 10 July 2025).

(c) Non-public domain (it must be information that is not publicly known).

In one notable case, a clothing manufacturer brought an action against a former employee for alleged misappropriation of trade secrets. After resigning from the company, the defendant promoted clothing products and related exhibitions through personal social media platforms. The plaintiff asserted that the clothing patterns used in the defendant's products constituted trade secrets belonging to the company.

However, the court held that the plaintiff failed to provide any detailed description or supporting documentation identifying the alleged trade secrets. Merely referencing product names and item numbers was deemed insufficient to establish the existence or characteristics of the trade secrets.[36]

As a result, the court dismissed the claim on the basis of insufficient identification of the trade secrets.

36 Tokyo District Court, Judgment rendered on 19 February 2024 Case No.2022 (Wa) 70057.

(9) Republic of Korea

1) Legal Framework

Republic of Korea governs the protection of trade secrets primarily under *the Unfair Competition Prevention and Trade Secret Protection Act (UTA)*. A trade secret is defined as information that

- Is not publicly known;
- Is economically value;
- Is subject to reasonable efforts to maintain confidentiality.

This includes technical or managerial information such as production methods, sales strategies, and other commercially useful data.

While the Act does not prescribe specific standards for the level of secrecy management, it is generally understood that a certain threshold of effort must be made to maintain confidentiality in order to satisfy the secrecy requirement.

2) Civil Remedies

Where trade secrets are infringed or there is a risk of infringement, the right holder may seek injunctive relief for prohibition or prevention of such acts. In addition, the court may order destruction of infringing products, removal of facilities used for infringement, and other necessary measures to prevent further misappropriation. In addition, where a trade secret holder's business reputation has been damaged as a result of a misappropriation committed intentionally or negligently, the injured party may seek appropriate measures from the infringer to restore such reputation.[37]

According to a 2022 study, former employees accounted for over 66.2% of civil trade secret misappropriation cases. Based on this finding, it is presumed that such misappropriation is more likely to be premeditated shortly before resignation rather than during active employment. In many instances, former employees are suspected of misappropriating trade secrets by establishing their own businesses after leaving the company or by disclosing the information to a competitor upon changing jobs.[38]

3) Criminal Remedies

Criminal liability arises when a person misappropriates a trade secret with the intent to gain unjust benefits or to cause harm to the rightful owner. This includes unauthorized acquisition, use, or disclosure to third parties; unauthorized export of trade secrets; and continued possession of trade secrets even after a return or deletion request by the owner.

Aggravated penalties apply if the trade secret is intended to be used abroad. Criminal sanctions also cover acts such as damaging, destroying, or altering trade secrets, and apply to attempts, preparatory acts, accomplices, and those who aid or abet such conduct.

---

37 Republic of Korea's *Unfair Competition Prevention and Trade Secret Protection Act (UTA)*, Articles 10(1), 10(2), and 12.

38 Jeong Kwan-Young et al., "2022 Trade Secret Protection Guide Study", KIPO & KOIPA (2022), p.22.

4) Economy-Specific Features

In cases where trade secrets constitute "Industrial technology", they are subject to separate regulation under *the Act on Prevention of Divulgence and Protection of Industrial Technology.* "Industrial technology" refers to technical information essential for the development, production, distribution, or use of products or services, designated by authorized agencies in accordance with industrial policy.

This Act was enacted to expand the scope of protection to technologies developed by public institutions, non-profit research entities, and universities—entities that often face practical limitations in satisfying the secrecy and non-disclosure requirements under the conventional trade secret regime. The significance of the Act lies in its role in enhancing the effectiveness of protecting internal core technologies by regulating the overseas transfer of internal core technologies that directly affect public security and by establishing institutional frameworks and promoting awareness to prevent the illicit leakage of industrial technologies.[39]

A key distinction lies in that industrial technologies under this Act do not need to be secret per se, nor do they require "independent economic value" as under trade secret law. Instead, their protection is justified based on specific policy objectives such as enhancing industrial competitiveness or preventing leakage of core technologies.[40]

5) Cases and Precedents

- ***Seoul Central District Court, Decision 2021Gahap525243, 11 October 2023***

The court found that while a software source code was not publicly known (satisfying the non-publicity requirement), it lacked independent economic utility and had not been properly managed as a secret. Thus, it did not qualify as a trade secret.

- ***Daejeon District Court, Decision 2023Godan2656, 1 February 2024***

A company had classified its trade secrets into categories such as "top secret," "important secret," and "general secret" based on internal security guidelines. The court recognized this effort as sufficient to meet the secrecy management requirement.

- ***Daejeon District Court, Decision 2022Gahap106228, 18 January 2024***

The court held that client contact details (e.g., names, emails, phone numbers) did not constitute information with independent economic value and thus did not qualify as trade secrets.

39 Kim Yong-Sup, "A Study on the Scope of Act on Prevention of Divulgence and Protection of Industrial Technology and Trade Secret Act", Hongik Law Review, Vol.19, No.4 (2018), p.592.

40 *Ibid.*

- ***Seoul Western District Court, Decision 2022Gadan277181, 28 May 2024***

Although the employee had received the password from a superior, the court found that this did not constitute authorization to access confidential trade secret files that had not been specifically requested. By logging in with the provided password and copying such files without instruction or consent, the employee engaged in tortious conduct. Accordingly, the court held the employee liable for damages.

- ***United States International Trade Commission, Decision in Investigation No. 337-TA-1159, 10 February 2021***

Although the decision was rendered in United States, both parties involved were Korean companies. The Commission found that SK Innovation had misappropriated LG Chem's trade secrets related to EV battery technology by hiring over 100 former LG employees and acquiring confidential information. The misappropriation violated Section 337 of the Tariff Act of 1930, leading to a ten-year limited exclusion order and cease and desist orders against SK Innovation.[41]

41 Matthew Rimmer, "Promethean Dreams: Intellectual Property and Climate Change in the Anthropocene", in Leonie Reins and Alexander Zahar (eds.), 'Climate Technology and Law in the Anthropocene', Bristol University Press (2023), pp.390–392. For the full text of the paper, please refer to the following website: https://ssrn.com/abstract=4557594 (last visit on 10 July 2025).

(10) Malaysia

1) Legal Framework and Recent Developments

Malaysia does not have a dedicated statute governing trade secrets. However, the concept of "confidential information" is referenced in *the Trademarks Act (TMA)*[42] and *Trade Descriptions Act (TDA)* primarily for the purpose of protecting sensitive information acquired during investigations or enforcement actions, rather than for general commercial trade secret protection. As such, this framework differs in nature from a typical trade secret protection regime.

Under *the Trade Marks Act*, "confidential information" refers to:[43]

(a) Trade, business, or industrial information belonging to any person;

(b) Information possessing economic value;

(c) Information not generally known or accessible to others; or

(d) Any information deemed confidential under the Act.

Infringement of confidential information" refers to the disclosure or use of confidential information or documents related to the business of a specific company or individual, obtained pursuant to the provisions of *the Trademarks Act*. However, the following cases shall not be considered as infringement.[44]

- Disclosure with the consent of the owner;
- Information structured in a way that prevents identification of the source;
- Information already in the public domain;
- Disclosure necessary for the functioning of enforcement officers;
- Disclosure in accordance with statutory procedures; or
- Disclosure related to the investigation of an offence under the Act.

Malaysian courts have consistently adopted the three-part test from *the English case Coco v. A.N. Clark (Engineers) Ltd [1969] RPC 41* in determining whether a breach of confidence has occurred. This approach was reaffirmed in the recent High Court case *CL Cosmetic Industries Sdn Bhd v. Syed Subri bin Syed Agil & Anor [2024] MLJU 1993*.

According to this test, a breach of confidence is established if;[45]

(a) The information is inherently confidential – it must not be trivial, commonplace, or publicly known. Widely used industry knowledge is not considered confidential.

---

42 Malaysia's *Trademarks Act 2019* (TMA 2019). For the original text of Malaysia's *Trademarks Act 2019*, please refer to the following website: https://www.wipo.int/wipolex/en/legislation/details/19564 (last visit on 14 July 2025).

43 Malaysia's *Trademarks Act*, Article 115(3).

44 Malaysia's *Trademarks Act*, Article 115(2).

45 Carmel Grace Philip, "Can I just Spill the Beans on my Employer's Trade Secrets? (Part 1)", Thomas Philip, Advocates & Solicitors (23 October 2024). For the original text of the article, please refer to the following website: https://www.thomasphilip.com.my/articles/can-i-just-spill-the-beans-on-my-employerrs-trade-secrets-part-1/ (last visit on 14 July 2025).

(b) There is an obligation of confidence – this may arise from an express confidentiality clause in an employment contract, or from implied duties of good faith and fidelity inherent in the employment relationship.

(c) The information is misused to the detriment of the owner – such misuse may involve disclosure to third parties or use for personal gain, resulting in commercial harm to the employer.

The CL Cosmetic Industries ruling reinforces that the confidential nature of the information, the existence of a duty, and the resulting harm are the key legal elements in trade secret disputes.

2) Civil Remedies

Malaysian courts may grant injunctions and damages in trade secret-related claims. Damages are generally assessed based on the loss of business profits caused by the defendant's conduct.

3) Criminal Remedies

While there is no standalone criminal provision specifically targeting trade secret misappropriation, *the Trademarks Act* criminalizes unauthorized disclosure or use of confidential information obtained under statutory authority.[46]

Malaysia does not have specific criminal provisions addressing trade secret misappropriation. However, where trade secrets are assumed to constitute "property," certain offenses under *the Penal Code* relating to property misappropriation may be applicable. In addition, penal provisions under other statutes, such as *the Computer Crimes Act* and *the Companies Act*, may potentially be applied to acts involving trade secret infringement.[47]

Under *the Computer Crimes Act*, criminal penalties may be imposed in cases where a person knowingly gains unauthorized access to a computer that is designed to perform functions for the purpose of protecting access to programs or data stored therein. The Act also provides for penalties where a person, who is not authorized to do so, directly or indirectly communicates any password, access code, or other means of access to the computer to another person.[48]

Under *the Companies Act*, directors or officers who misuse confidential company information, exploit business opportunities for personal gain, or engage in activities that compete with the company without shareholder approval, may be subject to fines or imprisonment.[49]

4) Economy-Specific Features

Malaysian courts generally do not consider post-resignation competitive conduct by former employees to be a breach of fiduciary duty. Utilization of general skills or industry knowledge acquired during employment is not protected by law. Only information that meets the legal threshold of "confidence" is eligible for protection.

---

46 Malaysia's *Trademarks Act*, Article 115(2).

47 Malaysia's *Penal Code*, Article 403. For the original text of the Malaysia's *Penal Code*, please refer to the following website: https://bwcimplementation.org/sites/default/files/resource/MY_Penal%20Code_EN.pdf (last visit on 14 July 2025).

48 Malaysia's *Computer Crimes Act*, Article 3. For the original text of the Malaysia's *Computer Crimes Act*, please refer to the following website: https://www.scribd.com/document/384940346/Act-563-Computer-Crimes-Act-1997 (last visit on 14 July 2025).

49 Malaysia's *Companies Act* (CA 2016), Article 218. For the original text of the Malaysia's *Companies Act* (CA 2016), please refer to the following website: https://www.scribd.com/document/709396531/Companies-Act-2016-Malaysia (last visit on 14 July 2025).

In *Vision Cast Sdn Bhd v. Dynacast (Melaka) Sdn Bhd [2014] 8 CLJ 884*, the court held that knowledge gained through years of industry experience did not qualify as confidential information.

Factors considered in determining whether information is confidential include:[50]

- The extent to which the information is known outside the business;
- The extent to which it is known within the business;
- Measures taken to guard the secrecy of the information;
- The value of the information to the business and competitors;
- The effort or cost required to develop the information;
- The ease with which others could acquire or duplicate the information independently.

5) Cases and Precedents

Malaysia lacks a statutory definition of "trade secret," and disputes are primarily adjudicated under common law principles and judicial precedents.

In *Faccenda Chicken Ltd v. Fowler*, the UK court distinguished between general confidential information and true trade secrets. It emphasized the importance of examining:[51]

- The nature of the employment relationship;
- The character of the information;
- Whether the employer impressed upon the employee the need for confidentiality;
- Whether the information was distinguishable from publicly available knowledge.

Following this approach, Malaysian employers are advised to clearly identify and document confidential information, particularly in employment contracts and internal policies.

In *Ecooils Sdn Bhd v. Raghunath Ramaiah Kandikeri*, the High Court found that a senior engineering executive had breached explicit contractual duties by disclosing confidential information to third parties. The court emphasized that express confidentiality obligations in employment contracts constitute independent and enforceable duties beyond implied fiduciary obligations.

In *Schmidt Scientific Sdn Bhd v. Ong Han Suan*, the court confirmed that confidentiality obligations continue after termination of employment. In *Dynacast (Melaka) Sdn Bhd v. Vision Cast Sdn Bhd*, the court further held that the duration of confidentiality protection may be either for a specific period—including one that extends beyond the termination of employment—or indefinite, depending on the terms of the agreement.[52]

---

50 *Electro Cad Australia Pty Ltd v Mejati RCS Sdn Bhd [2008] 4 CLJ 217*.

51 Drew Network Asia, "Malaysia: Trade Secret in Employment Perspective", Drew Network Asia Newsroom (27 July 2022). Please refer to the following website for the original version of the article: https://www.drewnetworkasia.com/newsroom/malaysia-trade-secret-in-employment-perspective/ (last visit on 14 July 2025).

52 Drew Network Asia, s*upra note 54*.

(11) Mexico

1) Legal Framework

In Mexico, trade secrets are regulated under the Federal Law on the Protection of Industrial Property (FLPIP), which was published in the Official Gazette on 1 July 2020, and entered into force on 5 November 2020.

According to Article 163 of the FLPIP, any industrial or commercial information kept confidential by a person exercising legal control over it, which provides or maintains a competitive or economic advantage over third parties, and for which adequate measures have been adopted to preserve confidentiality and restrict access, may qualify as a trade secret. However, the following types of information are excluded from trade secret protection;

- Information that is in the public domain;
- Information that is generally known or easily accessible to individuals within the circles where such information is normally used;
- Information that must be disclosed pursuant to legal provisions or court orders.

Misappropriation of trade secrets is defined as the acquisition, use, or disclosure of such information in a manner contrary to honest industrial, commercial, or service practices that involve unfair competition, including acquisition, use, or disclosure by a third party who knew or had reasonable grounds to know that the trade secret was obtained contrary to such practices.

Conversely, Article 164 of the FLPIP expressly excludes the following activities from being considered misappropriation.

- Independent discovery or creation of the information claimed as a trade secret;
- Observation, study, disassembly, or testing of a product or object that has been made publicly available or is lawfully in the possession of the person obtaining the information, provided that it is not subject to any confidentiality obligation;
- Lawful acquisition of the information from another person without a confidentiality obligation or without knowledge that the information constituted a trade secret.

Articles **386 (XIV and XV)** of the FLPIP establish the following as administrative infringements related to trade secrets:

XIV. Misappropriating information considered a trade secret without the consent of the person exercising legal control or its authorized user, to obtain a competitive market advantage or to engage in acts contrary to honest industrial, commercial, or service practices involving unfair competition;

XV. Producing, offering for sale, selling, importing, exporting, or storing products or services that use a trade secret, when the person carrying out such activities knew or had reasonable grounds to know that the trade secret was used without consent and in a manner contrary to honest practices involving unfair competition.

Administrative infringements will be processed and resolved in accordance with the administrative declaration procedure set forth in Title Six of the FLPIP and sanctioned under Article 388. Penalties will be determined based on intent, the infringer's economic conditions, the severity of the conduct, and the harm caused.

2) Civil Remedies

In Mexico, trade secret holders may also initiate civil proceedings to claim damages resulting from misappropriation.

When determining damages, courts may consider legitimate valuation indicators provided by the trade secret holder, including:

- The value of the infringing goods or services based on market price or suggested retail price;
- The profits the trade secret holder would have earned had the infringement not occurred;
- The gains obtained by the infringer as a result of misappropriation; or
- The commercial value of the infringed right, including the amount the infringer would have paid under a licensing agreement, considering any existing licenses.

3) Criminal Remedies

Criminal offenses related to trade secrets are set forth in Article 402 (sections III, IV, V, VI) of the FLPIP.

III. Disclosing a trade secret to a third party, obtained through employment, position, professional practice, business relationship, or under a license agreement, without consent and despite being warned of its confidentiality, for economic gain or to cause harm;

IV. Taking possession of a trade secret without right and without consent, to use or disclose it to a third party for economic gain or to cause harm;

V. Using information contained in a trade secret obtained through employment, position, professional practice, or business relationship, without consent, or disclosed by a third party without authorization, for economic gain or to cause harm;

VI. Misappropriating, acquiring, using, or unlawfully disclosing a trade secret by any means, without consent, to cause harm or obtain economic benefit for oneself or a third party.

Article 403 establishes penalties of two to six years of imprisonment and fines ranging from 1,000 to 300,000 units.

4) Economy-Specific Features

Under Article 163 of the FLPIP, a person exercising legal control over trade secret information must demonstrate that adequate measures or systems were implemented to preserve confidentiality and restrict access. While the law does not prescribe specific measures, these may vary depending on the nature of the trade secret and the entity's resources.

Common examples of protective measures include:

- Marking documents as "confidential";
- Executing confidentiality or non-disclosure agreements with individuals who have access to the information;
- Storing materials containing trade secrets in restricted-access or controlled areas;
- Using technical controls such as passwords, facial recognition, or fingerprint authentication.

Although there is no specific statute of limitations for civil actions related to trade secrets, the authority of the Mexican Institute of Industrial Property (IMPI) to impose administrative sanctions is subject to a five-year limitation period from the date of the infringing act.

5) Cases and Precedents

Recognized best practices for trade secret protection in Mexico include:

- Promoting a corporate culture of confidentiality and trade secret protection;
- Establishing internal policies defining what constitutes a trade secret;
- Setting internal authorization levels based on roles and responsibilities;
- Maintaining an internal inventory to identify key assets qualifying as trade secrets;
- Clearly marking all confidential and trade secret information;
- Executing confidentiality and non-disclosure agreements with all parties requiring access;
- Implementing sufficient systems and procedures to restrict access and preserve confidentiality.

Punitive damages may be claimed in cases of trade secret misappropriation, depending on the circumstances. In a relevant Supreme Court decision, punitive damages were described as:

"Punitive damages are exemplary sanctions with a preventive purpose, intended to deter the recurrence of similarly harmful conduct. Therefore, such remedies are only appropriate when the severity of the act justifies a high degree of social condemnation."

(12) New Zealand

1) Legal Framework

New Zealand protects trade secrets under its common law system, with criminal provisions also recognizing trade secret misappropriation. A trade secret generally refers to information that:[53]

- is or may be used industrially or commercially,
- is not generally known in industrial or commercial circles,
- is of actual or potential commercial value to the person possessing it, and
- is the subject of reasonable efforts to maintain its secrecy.

2) Civil Remedies

New Zealand does not have a specific statutory civil regime for the protection of trade secrets. Instead, protection is afforded under the equitable doctrine of breach of confidence, which derives from English common law.

Even in the absence of a formal contractual relationship, claims may be brought based on an obligation of confidence arising from the circumstances. New Zealand Court of Appeal has recognized the doctrine of confidence as a broad principle grounded in good faith.[54]

3) Criminal Remedies

Under Section 230(1) of *the Crimes Act*,[55] any person who, without proper authority and with intent to cause loss to another or to obtain a benefit for themselves, dishonestly takes, obtains, or copies any document, object, model, or schematic that contains or embodies a trade secret—knowing that it is a trade secret—may be liable for up to five years' imprisonment.

The provision also applies to persons who, with such intent and without proper authority, take or obtain a copy of such material, knowing that the reproduction contains or embodies a trade secret.

4) Economy-Specific Features

Under Section 52 of *the Privacy Act 2020*, access to personal information may be refused if it constitutes a trade secret.

Similarly, Section 9 of *the Official Information Act 1982* allows central agencies to withhold official information if its release would disclose a trade secret.

---

53 New Zealand's *Crimes Act 1961* (Version as at 5 April 2025), Article 230(2).

54 Rob Batty, "Trade Secrets' under New Zealand Law", SSRN Electronic Journal (2017), pp.13-14. Please refer to the following website for the full text of the paper: https://ssrn.com/abstract=2902349 (last visit on 14 July 2025).

55 New Zealand's *Crimes Act 1961* (Version as at 5 April 2025), Article 230(1).

5) Cases and Precedents[56]

New Zealand courts apply the elements established in the English case *Coco v A.N. Clark (Engineers) Ltd* to assess claims of breach of confidence. These elements are:

(a) The information must have the necessary quality of confidence,

(b) It must have been imparted in circumstances importing an obligation of confidence, and

(c) There must be an unauthorized use of that information to the detriment of the party communicating it.

These principles are generally adopted regardless of whether a contract exists.

New Zealand courts further consider the following factors in determining whether information qualifies as a trade secret:

- the originality of the information,
- the existence of commercial value,
- the effort and expertise required to create the information,
- the owner's perception of the information as confidential, and
- whether practical steps were taken to maintain its secrecy.

56 Rob Batty, s*upra note 57*, p.14.

(13) Papua New Guinea

1) Legal Framework

The legal system in Papua New Guinea is based on English common law. The two main sources of law are laws passed by Parliament ("Statutes") and "the underlying law" – law made by judges combining principles and rules of common law and equity in England as well as law derived from the customs of the various peoples of Papua New Guinea.[57]

In line with this framework, Papua New Guinea does not have a specific statute dedicated to the protection of trade secrets. Instead, trade secrets are governed by principles of common law and are adjudicated by courts on a case-by-case basis.

Trade secrets are generally understood as inventions, techniques, or information that are deliberately withheld from public disclosure to maintain a competitive advantage. In the local context, trade secrets may also include traditional knowledge such as medicinal uses of native plants, extraction techniques passed down through generations, biological classifications, and ecological information. Indigenous knowledge may be protected as trade secrets, particularly where communities enter into confidentiality agreements with third parties to secure economic benefits.

2) Civil Remedies

Papua New Guinea protects trade secret interests through the equitable doctrine of breach of confidence, derived from English common law, and through confidentiality obligations imposed under employment contracts.

3) Criminal Remedies

While Papua New Guinea does not have a dedicated criminal statute penalizing trade secret misappropriation, certain forms of wrongful acquisition and disclosure of information may be prosecuted under other laws:

- Under *the Protection of Private Communication Act 1973*,[58] any person who uses or enables the use of surveillance devices to intercept private communications may be subject to fines or imprisonment. This includes the disclosure or dissemination of such intercepted information to others, which is also punishable under the Act.
- Under *the Criminal Code Act*,[59] a person employed in public service who, by virtue of their position, improperly publishes or delivers secret documents or information in their custody may be punished with up to two years' imprisonment.[60]

---

57 UNCTAD, 'Gap Analysis of Cyberlaws in Pacific Small Island Developing States', United Nations (2025), p.60. For the original text of the UNCTAD report, please refer to the following website: https://unctad.org/system/files/official-document/dtlecde2024d6_en.pdf (last visit on 20 July 2025).

58 For the original text of Papua New Guinea's *Protection of Private Communication Act 1973*, please refer to the following website: https://www.paclii.org/pg/legis/consol_act/popca1973404/ (last visit on 14 July 2025).

59 For the original text of Papua New Guinea's *Criminal Code Act*, please refer to the following website: https://www.paclii.org/cgi-bin/sinodisp/pg/legis/consol_act/cca1974115/index.html?stem=&synonyms=&query=criminal (last visit on 14 July 2025).

60 Papua New Guinea's *Criminal Code Act*, Article 86.

4) Economy-Specific Features

Confidentiality clauses in employment contracts are commonly used to protect proprietary information, trade secrets, or business data. Such clauses are generally enforceable in Papua New Guinea provided they are reasonable in scope and duration.

5) Cases and Precedents

There are no publicly reported cases in Papua New Guinea specifically addressing trade secret misappropriation or breaches of confidentiality obligations.

(14) Peru

1) Legal Framework

In Peru, trade secrets are primarily governed by the following legal instruments:

- *Decision 486: Common Regime on Industrial Property of the Andean Community Commission*
- *Legislative Decree No.1075, which provides complementary provisions to Decision 486*
- *Legislative Decree No.1044: Law on the Repression of Unfair Competition*

According to these instruments, a trade secret is legally protected if it meets the following three cumulative conditions:

- it must be secret,
- it must have commercial value due to its secrecy, and
- it must be subject to reasonable measures to preserve its confidentiality.

The scope of protected information includes a wide range of business-related data such as the characteristics, properties, or uses of a product, manufacturing methods or processes, distribution channels, marketing strategies, and modes of service delivery.[61]

Legislative Decree No.1075 explicitly recognizes trade secrets as a component of industrial property.[62] Holders of trade secrets are granted legal protection against acquisition, use, or disclosure of such information when carried out through unfair commercial practices or without authorization.

The unauthorized acquisition, use, or disclosure of a trade secret constitutes an act of unfair competition under Peruvian law. Specific conduct deemed unlawful includes:[63]

- Using trade secrets without authorization in breach of confidentiality obligations arising from contractual or employment relationships.
- Disclosing or transmitting such information to third parties without consent, especially with the intent to benefit oneself or others or to harm the trade secret holder.
- Acquiring trade secrets through illegal means or in a manner contrary to honest commercial practices.
- Using, disclosing, or transmitting trade secrets obtained through unlawful methods.
- Utilizing trade secrets received from a third party, where the recipient knew or should have known that the third party had no legal authority to disclose them.

---

61 *Decision No.486* of the Andean Community Commission Establishing the Common Regime on Industrial Property, Article 260. Please refer to the following website for the full text of *Decision No.486* of the Andean Community Commission Establishing the Common Regime on Industrial Property: https://www.ampeid.org/documents/regional/decision-no-486-of-the-andean-community-commission-establishing-the-common-regime-on-industrial-property/#:~:text=Decision%20486%20establishes%20the%20new%20legal%20framework%20for,all%204%20Member%20States%20of%20the%20Andean%20Community. (last visit on 2 July 2025).

62 Peru's *Legislative Decree No.1075*, Article 3. Please refer to the following website for the full text of Peru's *Legislative Decree No.1075*: https://cdn.www.gob.pe/uploads/document/file/1664721/DL%201075.pdf.pdf?v=1613011875 (last visit on 2 July 2025).

63 *Decision No.486* of the Andean Community Commission Establishing the Common Regime on Industrial Property, Article 262.

- Disclosing or transmitting such misappropriated trade secrets to benefit oneself or others or to damage the trade secret holder.

Examples of acts contrary to honest commercial practices include industrial espionage, breaches of contractual or legal obligations, violations of fiduciary duties or duties of loyalty, and instigating or inducing others to commit such acts.

Legislative Decree No.1044 also categorizes unauthorized acquisition, use, and disclosure of trade secrets as unfair competition and provides a detailed list of such prohibited behaviours.

2) Civil Remedies

In cases of trade secret misappropriation, the rights holder may request interim measures aimed at stopping the infringement, preserving evidence, or facilitating legal actions for damages. The precautionary measures are intended to ensure the effectiveness of the final decision, which includes ensuring compliance with corrective measures and the collection of any sanctions that may be imposed. Article 33.2 of *Legislative Decree No.1044* establishes that interim measures may include:

It should be noted that, in Peruvian legislation, precautionary measures are ordered by the administrative authority within the framework of an administrative sanctioning procedure.

Article 33.2 of *Legislative Decree No.1044* establishes that interim measures may include:

- Ensuring compliance with corrective measures and the collection of any applicable penalties.
- Issuing a cease and desist order or a prohibition on the act if it has not yet been implemented.
- Imposing conditions, confiscating, impounding, or immobilizing the products, labels, packaging, and advertising material that are the subject of the complaint.
- Taking the necessary measures to ensure that customs authorities prevent the entry into the country of the products that are the subject of the complaint, which must be coordinated with the competent authorities in accordance with current legislation.
- Temporarily closing the establishment of the accused party, encouraging positive actions, and taking any other measures that contribute to preserving fair competition and preventing the harm that the acts subject to the proceedings could cause.

In addition, Article 55.1 of *Legislative Decree No.1044* establishes that corrective measures may include;

- The cessation of the act or its prohibition if it has not yet been implemented.
- The removal of the effects produced by the act, through the performance of activities, including under specific conditions.
- The seizure and/or destruction of products, labels, packaging, infringing material, and other elements of false identification.
- The temporary closure of the infringing establishment.
- The correction of misleading, incorrect, or false information.
- The adoption of necessary measures to ensure that customs authorities prevent the entry into the country of products subject to infringement, which must be coordinated with the competent authorities in accordance with current legislation.
- The publication of the condemnatory resolution.

3) Criminal Remedies

While Article 222 of *the Criminal Code* addresses industrial property infringements, it does not appear to explicitly cover trade secret misappropriation.[64]

With respect to trade secrets, Article 165 of the Criminal Code stipulates that a person who, by reason of their position, employment, profession, or public office, becomes aware of confidential information that may cause harm if disclosed and subsequently reveals such information without the consent of the concerned party shall be subject to a fine or imprisonment.[65] However, this provision primarily targets the unauthorized disclosure of professional secrets and does not specifically regulate trade secrets as defined under industrial property law.

Therefore, Peru does not currently have a distinct or comprehensive criminal provision that directly addresses trade secret misappropriation in the context of commercial or competitive behaviour.

4) Economy-Specific Features

No specific features or distinctive trends concerning trade secrets have been identified in Peru.

5) Cases and Precedents[66]

In late 2020, Peru's Institute for the Defense of Competition and Protection of Intellectual Property (INDECOPI), through its Chamber for the Defense of Competition (Sala Especializada en Defensa de la Competencia), issued notable decision finding APC Corporación liable for misappropriating trade secrets from its competitor, Sodexo Perú.

The case involved commercial espionage wherein a senior executive at APC gained unauthorized access to Sodexo's email accounts and extracted confidential business information. The stolen data provided APC with an undue competitive advantage in a public procurement process.

INDECOPI concluded that the conduct constituted both a clear violation of trade secret protection and an act of unfair competition (espionaje corporativo).

---

64 Peru's *Legislative Decree No.635*, Article 222 (Unauthorized Manufacture or Use of a Patent)

Anyone who, in violation of industrial property regulations and rights, stores, manufactures, uses for commercial purposes, offers, distributes, sells, imports, or exports, in whole or in part, shall be punished with imprisonment for not less than two years and not more than five years, a fine ranging from sixty to three hundred sixty-five days, and disqualification in accordance with Article 36, paragraph 4, taking into account the seriousness of the offense and the value of the harm caused:

a) A product protected by a patent of invention or a product manufactured using a process protected by a patent of invention granted in the economy;

b) A product protected by a utility model granted in the economy;

c) A product protected by a registered industrial design in the economy;

d) A registered plant variety in the economy, including its reproductive, propagation, or multiplication material;

e) A registered layout design (topography) in the economy, a semiconductor circuit incorporating such layout design, or an article incorporating such semiconductor circuit;

f) A product or service that uses an unregistered mark identical or similar to a registered trademark in the economy.

65 Peru's *Legislative Decree No.635*, Article 165.

66 Agustín Valencia-Dongo, "Espionaje corporativo en el Perú: el caso del ejecutivo topo", Bullard Falla Ezcurra (1 May 2021). Please refer to the original text of the article at the following website: https://bullardfallaezcurra.com/boletin/2021/05/04/espionaje-corporativo-en-el-peru-el-caso-del-ejecutivo-topo/ (last visit on 2 July 2025).

Although INDECOPI had investigated over 20 trade secret-related cases in the previous 12 years, most were dismissed due to insufficient evidence, and only one had previously resulted in a decision favouring the claimant—and even that case involved mere inadvertent disclosure rather than deliberate corporate espionage. The APC case stands out as a rare instance in which commercial espionage was explicitly sanctioned as trade secret misappropriation under Peruvian law.

A key factor in substantiating the violation was digital forensic analysis, which confirmed multiple unauthorized remote accesses to Sodexo's email systems from APC-owned devices. This technical evidence was critical in supporting the decision. This demonstrates that in trade secret cases, where proof is often difficult to obtain, technical evidence can play a pivotal role in the adjudication.

Importantly, INDECOPI held the company (APC) responsible, not just the individual employee, reasoning that the employee's actions were carried out for the benefit of the company. This case set a precedent for potential corporate liability arising from the unlawful conduct of its executives.

(15) The Republic of the Philippines

1) Legal Framework and Recent Developments

The Republic of the Philippines does not have a standalone statute dedicated to trade secrets. However, confidential business information is defined and recognized in several laws concerning intellectual property and competition.

Under the Philippines' law, trade secrets—referred to as confidential business information—may include data related to operations, production, sales, shipments, purchases, transfers, customer identification, inventories, and financial records such as revenues, profits, and losses.[67]

In *Air Philippines Corp. v. Pennswell, Inc. (G.R. No. 172835, 13 December 2007)*, the Supreme Court clarified that a trade secret refers to a plan, process, tool, mechanism, or compound known only to the owner and a limited number of trusted employees. The definition encompasses non-patented formulas and processes that provide commercial advantage and are not generally known to competitors.

Thus, the concept of trade secrets in The Republic of the Philippines encompasses not only mechanical or chemical formulas, but also operational procedures, pricing models, proprietary catalogues, and customer lists, provided that such information is not publicly known and confers a competitive advantage.[68]

The Republic of the Philippines legal system uses three core criteria in determining whether information qualifies as a trade secret: non-publicity, commercial value, and limited disclosure within a relationship of trust. This is broadly consistent with international principles.

2) Civil Remedies

Trade secrets can be protected through contractual obligations or judicial enforcement. Confidentiality clauses are commonly included in employment and service agreements. A breach of such agreements may result in civil liability for damages.[69]

Under Article 1314 of *the Civil Code*, third parties who knowingly induce a breach of contract may also be held liable. To invoke this article, the plaintiff must prove that a valid contract existed, that the third party had knowledge of the contract, and that the third party interfered without legal justification.

3) Criminal Remedies

The Competition Act prohibits the unauthorized disclosure, publication, transmission, or distribution—whether directly or indirectly—of confidential business information submitted to the competent authorities. Violations may result in fines.[70]

---

67 *The Competition Act*, Article 4(e). For the original text of the Philippine *Competition Law*, please refer to the following website: https://www.phcc.gov.ph/file-manager/1/About%20Us/Philippine-Competition-Act-PCA-1.pdf (last visit on 2 July 2025).

68 For more detailed information on the protection of trade secrets in The Republic of the Philippines, please refer to the following website: https://vietanlaw.com/learn-about-trade-secrets-in-the-philippines/ (last visit on 2 July 2025).

69 *The Civil Code*, Article 1170.

70 *The Competition Act*, Article 34.

The Revised Penal Code, under Article 292, provides criminal sanctions for the unauthorized disclosure of industrial secrets by persons working in a manufacturing or industrial establishment if such disclosure causes harm to the owner. Penalties include imprisonment or fines.

4) Economy-Specific Features[71]

Trade secrets are considered a form of intellectual property in the Republic of the Philippines, and Non-Disclosure Agreements (NDAs) serve as a key mechanism for their protection.

NDAs are widely used in commercial transactions and employment relationships to prevent the unauthorized disclosure of proprietary information. For an NDA to be enforceable:

- Mutual consent must be present, free from fraud, mistake, or undue influence.
- The object of the contract must be lawful and specific; information must be clearly defined and confidential in nature.
- The obligation must be reasonable in scope, duration, and geography.
- The NDA must not unduly restrain trade or violate public policy.

Courts balance the employer's right to protect legitimate business interests with the employee's right to livelihood. Overly broad or indefinite confidentiality obligations may be held unenforceable.

NDAs must also be narrowly tailored to cover only confidential information. Courts of the Philippines may invalidate NDAs that attempt to cover publicly available information or information unrelated to the employment relationship.

The duration of confidentiality must be reasonable. While trade secrets may merit longer protection periods, the court may reject perpetual confidentiality clauses unless justified by the nature of the information. Geographic restrictions are rare in Philippine NDAs but may be valid in industries with clear market segmentation.

5) Cases and Precedents

The Republic of the Philippines jurisprudence on trade secrets has consistently emphasized the confidentiality of such information and the necessity of its protection

In *Garcia v. Board of Investments*, the Supreme Court held that trade secrets and confidential commercial or financial information are exempt from disclosure obligations. This principle was reaffirmed in *Chavez v. Presidential Commission on Good Government*, where the Court clarified that even in cases involving mandatory document production or information disclosure, trade secrets in the possession of a party remain protected and are not subject to compulsory disclosure.

71 Harold Respicio, "Legality of Non-Disclosure Agreements in Employment Contracts in the Philippines", Legal consultation posted on Lawyer-Philippines.com (5 October 2024). Please refer to the following website for the original text of the article: https://www.lawyer-philippines.com/articles/legality-of-non-disclosure-agreements-in-employment-contracts-in-the-philippines (last visit on 2 July 2025).

In *Air Philippines Corp. v. Pennswell, Inc*., the Court broadly defined trade secrets to include confidential formulas, mechanisms, and internal processes that are not patented but confer a competitive advantage due to their secrecy. The Court emphasized that trade secrets are a form of property and must be protected accordingly.

The Court also referred to the case law of United States, identifying key factors in assessing whether information qualifies as a trade secret:

- The extent of public knowledge about the information;
- Internal dissemination within the company;
- Measures taken to safeguard secrecy;
- The information's economic value and competitiveness;
- Resources invested in its development;
- Ease of replication or independent discovery by others.

These standards serve as the basis for evaluating whether a party has met the "substantial factual basis" required to assert trade secret protection.

In *Cocoland Development Corp. v. National Labour Relations Commission*, the Supreme Court ruled that the employer's mere assertion that certain information constituted a trade secret was insufficient. The Court emphasized the need for objective and substantial evidence, warning against the misuse of trade secret claims to justify employee termination.

In conclusion, the Philippine Supreme Court affirms the importance of protecting trade secrets while demanding judicial scrutiny and evidentiary rigor to prevent abuse. Companies seeking protection must clearly identify the trade secret and demonstrate its proprietary nature.[72]

72 Rogelio Nicandro & Juan Carlos Novero, "Trade secrets in the Philippines protected by blend of laws", Law.asia (2 May 2025). For the original text of the article, please refer to the following website: https://law.asia/trade-secret-laws-philippines-taiwan-legal-trends/ (last visit on 2 July 2025).

(16) The Russian Federation

1) Legal Framework[73]

Trade secrets in the Russian Federation are primarily governed by:[74]

- *Civil Code of the Russian Federation* (Part IV, Chapter 75);[75]
- *Federal Law No. 98-FZ of 29 July 2004, on Trade Sec*rets (the "Trade Secret Law");[76]
- *Federal Law No. 135-FZ of 26 July 2006, on the Protection of Competition*;[77] and
- *Criminal Code of the Russian Federation*.[78]

Article 1465(1) of *the Civil Code* defines a manufacturing secret (know-how) as information of any nature—production, technological, economic, organizational, or otherwise—relating to the results of intellectual activities in science and technology, or to methods of conducting professional activities. The information must:

- Have actual or potential commercial value due to its secrecy;
- Not be generally known or accessible to third parties on a lawful basis; and
- Be subject to reasonable measures for confidentiality protection, particularly through the implementation of a trade secret regime.

Pursuant to Article 1465(2), data required to be disclosed by law or other legal acts, or data for which access may not be restricted, shall not be deemed trade secrets.

The Trade Secret Law (Article 10(1)) outlines the minimum protective measures that trade secret holders must implement, including:

- Establishment of a list of information classified as trade secrets;
- Restriction of access through defined handling procedures and compliance monitoring;
- Maintenance of records identifying individuals who accessed, received, or were transferred the information;

---

73 World Intellectual Property Organization, "Overview of National and Regional Trade Secret Systems: Russian Federation", WIPO (2024). Please refer to the following WIPO website for the original text of the research: https://www.wipo.int/documents/d/trade-secrets/docs-overview-country-sheets-russian-fed-final.pdf (last visit on 14 July 2025).

74 For further information on the Trade Secret Protection System in Russia, please refer to the following articles: Evgeny Alexandrov and Ilya Goryachev, "Trade Secrets – Russia", les Nouvelles - Journal of the Licensing Executives Society, Volume LVI No.2 (June 2021). Please refer to the following website for the full text of the paper: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3832155 (last visit on 14 July 2025).

75 Please refer to the following WIPO website for the full text of *the Civil Code of the Russian Federation*: https://www.wipo.int/wipolex/en/legislation/details/22547 (last visit on 14 July 2025).

76 Please refer to the following WIPO website for the full text of the Russian *Federal Law No.98-FZ of 29 July 2004, on Trade Secrets* (as amended up to Federal Law No.35-FZ of 12 March 2014): https://www.wipo.int/wipolex/en/legislation/details/15707 (last visit on 14 July 2025).

77 Please refer to the following WIPO website for the full text of *the Russian Federal Law No.135-FZ of 26 July 2006, on the Protection of Competition* (as amended up to Federal Law No.11-FZ of 17 February 2021): https://www.wipo.int/wipolex/en/legislation/details/20816 (last visit on 14 July 2025).

78 Please refer to the following WTO website for the full text of *the Criminal Code of the Russian Federation*: https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_362.pdf (last visit on 14 July 2025).

- Regulation of trade secret usage via employment and civil contracts;
- Labelling of physical or documentary materials with a "Trade Secret" stamp, including the identity of the information holder.

Under Article 1466(1) of *the Civil Code*, a trade secret confers an exclusive right to use the information in any lawful manner, in accordance with Article 1229 of *the Civil Code*. This includes the right to use the information in manufacturing processes or organizational decisions, and to assign or license such rights.

According to Article 1466(2), an individual who has independently and in good faith obtained access to trade secret information—without infringement of the rights of another holder—acquires an independent exclusive right to use that production secret.

2) Civil Remedies[79]

Pursuant to Article 14(1) of *the Trade Secret Law*, the violation of trade secret regulations may result in disciplinary, civil, administrative, or criminal liability under the legislation of the Russian Federation.

Under Article 1472 of *the Civil Code*, a trade secret holder may bring a civil damage claim in cases involving unauthorized use, disclosure, or dissemination of exclusive rights to a production secret (know-how). Furthermore, Article 6.1(6) of *the Trade Secret Law* affirms that the right holder may seek legal protection in response to the disclosure, illegal acquisition, or unauthorized use of trade secret information by third parties, including the right to claim compensation for damages resulting from such violations.

In civil proceedings, the claimant is required to:

- Demonstrate ownership of the trade secret;
- Prove the confidential nature of the information; and
- Provide evidence of the defendant's unauthorized activities, including use, disclosure, dissemination, or use of the information beyond the scope of contractual obligations.

Under the general statute of limitations, an action for breach of confidential information must be initiated within three years from the date when the claimant became aware, or should have become aware, of the infringement and the identity of the infringer.

3) Criminal Remedies[80]

According to Article 183 of *the Criminal Code of the Russian Federation*, the following acts constitute criminal offenses related to trade secrets:

- The unlawful acquisition of trade secret information through means such as bribery, theft of documents, intimidation, or other illegal methods; and
- The unauthorized disclosure or use of information constituting a commercial secret.

Depending on the severity and specific circumstances of the offense, criminal penalties may include fines, corrective labour, or imprisonment. The applicable punishment is determined by the nature of the offense, the method used, and the resulting harm to the trade secret holder.

---

79 World Intellectual Property Organization, *supra note 77*.

80 *Ibid.*

4) Economy-Specific Features

Under the Russian Federation law, employees who have access to trade secrets in the course of their employment may be held disciplinarily liable if they intentionally breach trade secrecy or disregard confidentiality measures. Disciplinary sanctions may include warnings, reprimands, or dismissal.

An employee's monetary liability for trade secret violations is generally limited to actual damages that are directly and realistically incurred. These include:

- Loss or deterioration of the employer's property;
- Expenses incurred to restore or replace such property; and
- Compensation paid by the employer to third parties for damage caused by the employee's actions.

However, expected profits or anticipated gains lost by the employer as a result of the trade secret breach cannot be claimed against the employee. In principle, the employee's liability for damages is limited to an amount not exceeding their average monthly wage, unless otherwise provided by law.

In cases of dismissal due to a trade secret breach, the Supreme Court of the Russian Federation requires the employer to prove;[81]

(a) That the leaked information qualifies as a trade secret protected under applicable law;
(b) That the employee had access to the information through their official duties; and
(c) That the employee was aware that such disclosure to third parties was prohibited.

As a result, the civil liability of employees for trade secret violations is considerably limited in the Russian Federation, and it may be difficult for employers to obtain effective protection due to the burden of proof regarding intent, harm, and procedural requirements.

5) Cases and Precedents

According to a judicial review report[82] on disputes related to breach of non-disclosure agreements (NDAs) in the Russian Federation between 2018 and 2020, the number of NDA-related disputes in 2020 increased by 32% compared to 2018. The total amount recovered in civil proceedings over the three-year period exceeded RUB 14 million, with civil lawsuits accounting for 58.2%, administrative proceedings 8.5%, and criminal proceedings 33.3% of all cases.

Typical examples of trade secret breaches included:

- Former employees disclosing know-how or other confidential business or industrial information;
- Attorneys disclosing confidential information about their clients; and
- Contracting parties disclosing trade secrets obtained in the course of contractual performance.

---

81 Law Library of Congress, 'Protection of Trade Secrets: Brazil, China, India, Russian Federation, South Africa', Create Space Independent Publishing Platform (2014), pp.18-19. Please refer to the following website for the full text of the report: https://sgp.fas.org/eprint/lloc-trade.pdf (last visit on 14 July 2025).

82 RTM Group, 'Анализ судебной практики за 2018-2020 годы по спорам, связанным с нарушением NDA (соглашение о неразглашении)', RTM Group (2021). Please refer to the following website for the original text of the report: https://rtmtech.ru/research/analiz-sudebnoj-praktiki-za-2018-2020-po-sporam-s-narusheniem-nda/ (last visit on 2 July 2025).

Courts have occasionally ruled in favour of employees even when serious breaches of duty, such as the disclosure of trade secrets acquired through their work, were alleged. In particular, dismissals were ruled unlawful where:

- The employer failed to prove that the employee disclosed information that legally qualified as a trade secret;
- The NDA signed by the employee did not include a specific list of information prohibited from disclosure;
- The employee was not sufficiently informed about what information constituted a trade secret, or about the confidentiality regime and legal consequences of a breach.

However, when the employer successfully demonstrated that a trade secret protection regime had been established within the organization, that the employee was aware of the specific information not to be disclosed in the course of their duties, and that the employee understood the legal consequences of breaching the confidentiality regime, the dismissal was upheld as lawful.[83]

83 RTM Group, *supra note 86*.

(17) Singapore

1) Legal Framework

Singapore does not have a specific statute governing trade secrets. Instead, trade secrets are protected under common law, particularly through the law of confidence. To qualify for such protection, three elements must be satisfied:

(a) The information must possess the necessary quality of confidence (i.e., it is not publicly known);

(b) The information must have been imparted in circumstances importing an obligation of confidence, which may arise through contractual means (e.g., employment contracts or NDAs) or equitable obligations (e.g., password-protected files);

(c) There must have been an unauthorized use or disclosure of the information to the detriment of the party communicating the confidential information, or where the information was not used or disclosed, the defendant is unable prove that their conscience was unaffected.

In exceptional circumstances, a defendant may invoke a public interest defense to justify the disclosure of otherwise confidential information. When a breach of confidence is established, remedies available include injunctions, monetary compensation (damages or an account of profits), and orders for delivery-up or destruction of materials containing the confidential information.[84]

2) Civil Remedies

Trade secret holders may seek injunctive relief, monetary compensation, or court orders for the delivery-up or destruction of documents containing trade secrets.[85]

In Singapore, a breach of contract related to confidential information—such as unauthorized use or disclosure of trade secrets—may constitute a breach of confidence.[86] Courts assess whether the information possesses sufficient confidentiality, whether it was disclosed under circumstances giving rise to a duty of confidentiality (either contractually or impliedly), and whether the information was used or disclosed to the detriment of the owner of confidential information.

The Singapore Court of Appeal has recognized the difficulties encountered by owners of confidential information in proving that such information was used by the defendant and thus, formulated a modified test for cases where is no use or disclosure of the information. In such cases, if it is shown that information was confidential and imparted in circumstances importing an obligation of confidence, breach is presumed and the burden is placed on the defendant to prove that its conscience was not affected.[87] Possible defenses include accidental exposure, lack of awareness of the information's confidential nature, or disclosure being justified in the public interest.

---

84 Ivy Liang, "How to protect your trade secrets in South-East Asian economies and China", Gowling WLG (18 January 2023). Please refer to the following website for the original text of the article: https://gowlingwlg.com/en/insights-resources/articles/2023/trade-secret-protection-in-sea-and-china (last visit on 14 July 2025).

85 Sheena Jacob, "Trade secret laws and regulations in Singapore", CMS Expert Guide to Trade Secrets (18 May 2022). Please refer to the original text of the article at the following website: https://cms.law/en/int/expert-guides/cms-expert-guide-to-trade-secrets/singapore (last visit on 14 July 2025).

86 *Obegi Melissa and Others v Vestwin Trading Pte Ltd and Another [2008] 2 SLR(R) 540*.

87 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others [2020] SGCA 32*.

Where a breach of confidence has been made out, restitutionary remedies may be awarded. In such cases, the defendant may be required to account for the net profits derived from the breach of confidence. Courts may also award equitable compensation to the claimant. The appropriate compensation will be determined by the courts on a case-by-case basis, and some factors which have been considered in past cases include:

(a) the additional costs the defendant would have incurred to develop the product independently without access to the claimant's materials; and

(b) the time advantage or early revenue generation resulting from an accelerated market entry.[88]

Claims for breach of confidence must be brought within six years from the date the cause of action arose, or within three years from the time the claimant first possessed the knowledge and right to commence proceedings—whichever expires later.

3) Criminal Remedies

Although Singapore law does not criminalize trade secret misappropriation per se, *the Computer Misuse Act 1993* provides for penalties against unauthorized access to computer programs or data. A person who accesses, views, copies, or extracts information from systems or servers without authorization may be liable for a fine and/or imprisonment.[89]

Furthermore, if such access was carried out with intent to cause wrongful loss, commit fraud, or gain unlawful advantage, more severe penalties may apply.[90] Sharing access credentials with unauthorized individuals—knowing the risks of misuse—may also trigger criminal liability.[91] Accordingly, the unauthorized disclosure or transfer of access credentials to systems that store trade secrets to third parties may constitute a criminal offense under applicable provisions, as it may be deemed a violation of confidentiality obligations and unauthorized access to protected information.

4) Economy-Specific Features

To ensure trade secrets and confidential information are protected under Singapore law, owners must implement reasonable protective measures. These may include:

- Restricting access to trade secrets to a defined group of employees (e.g., management);
- Keeping records of all transactions involving trade secrets and clearly marking such information as "confidential";
- Executing NDAs or confidentiality clauses with all persons granted access to trade secrets (e.g., employees, consultants, suppliers).

Singapore also recognizes the Riddick Principle, whereby documents disclosed during discovery proceedings are subject to an implied undertaking that they will not be used for purposes other than the litigation itself (see *Riddick v Thames Board Mills Ltd [1977] QB 881*).

---

88 *I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others [2020] SGCA 32*.

89 Singapore's *Computer Misuse Act 1993*, Article 3 (Unauthorised access to computer material). For the original text of Singapore's *Computer Misuse Act 1993*, please refer to the following website: https://sso.agc.gov.sg/Act/CMA1993 (last visit on 14 July 2025).

90 Singapore's *Computer Misuse Act 1993*, Article 4 (Access with intent to commit or facilitate commission of offence).

91 Singapore's *Computer Misuse Act 1993*, Article 7 (Unauthorised obstruction of use of computer).

5) Cases and Precedents

In *I-Admin (Singapore) Pte Ltd v Hong Ying Ting and others* [2020] SGCA 32, the Court of Appeal established a modified test for breach of confidence to protect claimants' interests where confidential information has been wrongfully acquired but not necessarily used. They termed this the "wrongful loss" interest, a claimant's interest in avoiding wrongful loss of confidentiality. Under the modified approach, once it is shown that information is confidential and was imparted in confidence, a breach is presumed. The burden then shifts to the defendant to prove that their conscience is not negatively affected by their acquisition of confidential information.

Subsequent cases have clarified that both the traditional and modified approaches are valid in Singapore law and may be relied upon within the same action for breach of confidence, provided the claims are not made in respect of the same documents.[92]

In the employment context, employees generally owe a duty of confidentiality to their employers. Upon termination of the employment relationship, the ex-employee cannot use or disclose the trade secrets of his ex-employer. To assess if such information qualifies as a trade secret, courts assess factors such as:[93]

- The nature of the employment;
- The characteristics of the information;
- Whether the employer emphasized the confidential nature of the information; and
- Whether the information can be easily distinguished from publicly available knowledge.

Disclosure of a trade secret without the owner's consent may be justified only when required by overriding public interest.[94]

92 *Centricore (S) Pte Ltd v ATT Systems (S'pore) Pte Ltd [2025] SGHC(A) 17*

93 *Man Financial (S) Pte Ltd v Wong Bark Chuan David [2007] SGCA 53*.

94 *X Pte Ltd and another v CDE [1992] SGHC 229*.

(18) Chinese Taipei

1) Legal Framework

Chinese Taipei regulates trade secrets under its standalone *Trade Secrets Act (TSA)*.[95]

Under Article 2 of the Act, a trade secret refers to information—including methods, techniques, processes, formulas, programs, designs, or other data—that

(a) is not known to persons generally involved in the information of this type;

(b) has economic value, actual or potential, due to its secretive nature; and

(c) is subject to reasonable measures for maintaining secrecy.

Such information shall be usable in production, sales, or other business activities.

Article 10 of the Act defines trade secret misappropriation as including the following:

- Acquiring trade secrets through improper means;
- Acquiring, using, or disclosing trade secrets knowingly or unknowingly due to gross negligence;
- Using or disclosing trade secrets knowing (or gross negligence in failing to know) that they were acquired through improper means;
- Improperly using or disclosing trade secrets even if they were lawfully acquired;
- Using or disclosing trade secrets without legitimate reason despite a statutory obligation to protect them.[96]

Improper means include theft, fraud, coercion, bribery, unauthorized duplication, breach of confidentiality obligations, and inducement of others to breach such obligations.[97]

2) Civil Remedies

A person who intentionally or negligently infringes on another's trade secret is liable for damages. If multiple parties jointly commit the infringement, they bear joint and several liability. Claims must be filed within 2 years from on which the owner of the trade secrets becomes aware of both the act of misappropriation and the identity of the party liable for the damage, and no later than 10 years from the date of the infringing act.[98]

If the plaintiff cannot prove actual damages, courts may presume the damage to be the difference between the expected profit under normal use of the trade secret and the actual profit earned after infringement. In cases of wilful infringement, punitive damages may be awarded based on the severity of the conduct, up to three times the proven amount of damages.[99]

---

95 For the original text of Chinese Taipei's *Trade Secrets Act*, please refer to the following website: https://law.moea.gov.tw/EngLawContent.aspx?id=10372 (last visit on 20 July 2025).

96 Chinese Taipei's *Trade Secrets Act*, Article 10.

97 Chinese Taipei's *Trade Secrets Act*, Article 10.

98 Chinese Taipei's *Trade Secrets Act*, Article 12.

99 Chinese Taipei's *Trade Secrets Act*, Article 12.

3) Criminal Remedies

Where a person misappropriates trade secrets to gain unlawful benefits for themselves or a third party, or to harm the trade secret holder, criminal penalties including fines and imprisonment may apply. Attempted misappropriation is also punishable. When the benefit gained by the offender exceeds the statutory maximum fine, the court may impose a fine of up to three times the unlawful gain. This enhanced penalty reflects a punitive approach within the criminal framework, intended to deter wilful misappropriation by targeting the economic advantage obtained.[100]

In cases the offense is committed with the intent of using the trade secret in foreign jurisdictions, mainland China; Hong Kong, China; or Macau, the offender may be sentenced to up to 10 years' imprisonment. If the benefit gained exceeds the standard fine, the court may impose an enhanced fine of two to ten times the benefit obtained.[101]

Chinese Taipei adopts a distinctive structure in which criminal fines are linked to the amount of unlawful gain. In addition, trade secret misappropriation under Article 13-1 is classified as a complainant-driven offense, requiring a formal complaint by the rights holder for prosecution to proceed.[102]

4) Economy-Specific Features

Chinese Taipei adopts an intellectual property perspective in regulating trade secrets, including specific provisions concerning ownership rights. Where trade secrets are jointly developed by multiple parties, ownership is determined according to contractual agreement. In the absence of such an agreement, equal co-ownership is presumed. If the trade secret is jointly owned, all co-owners must consent to its use or disposal, unless otherwise agreed. However, no co-owner may unreasonably withhold consent.[103]

Furthermore, trade secrets of foreign individuals or entities are not protected in Chinese Taipei under the following conditions:[104]

- The other economy has not concluded any international treaty for the protection of trade secret(s) with Chinese Taipei;
- There is no bilateral or multilateral agreement on mutual trade secret protection;
- The other economy does not provide equivalent protection for residents or entities of Chinese Taipei.

5) Cases and Precedents

In July 2024, the Intellectual Property Office of the Ministry of Economic Affairs published a compilation of judicial decisions to promote understanding of trade secret jurisprudence. The report surveyed 67 civil and criminal judgments rendered by various courts, selecting 22 significant cases deemed particularly instructive. The following summarizes the principal case names as presented in the source material.[105]

---

100 Chinese Taipei's *Trade Secrets Act*, Article 13-1.

101 Chinese Taipei's *Trade Secrets Act*, Article 13-2.

102 Chinese Taipei's *Trade Secrets Act*, Article 13-3.

103 Chinese Taipei's *Trade Secrets Act*, Article 6.

104 Chinese Taipei's *Trade Secrets Act*, Article 15.

105 For more detailed information on trade secret-related cases in Chinese Taipei, please refer to the following website: https://www.tipo.gov.tw/tw/cp-7-976337-4e186-1.html (last visit on 10 July 2025).

Non-publicity and Economic Value

- Real estate "reserve price" can be obtained through various channels, such as online searches or inquiries with the community manager, and therefore lacks secrecy. (18 January 2023)
- Supplier list does not involve any confidential information regarding business dealings or technologies between the complainant's company and other companies, and therefore lacks secrecy. (29 March 2023)
- The rice ball sauce recipe and its proportions are not readily known to other rice ball businesses, and if obtained, could potentially harm the plaintiff's competitive advantage. It therefore possesses secrecy and economic value. (19 April 2023)
- Human clinical test data was denied trade secret status due to failure to meet criteria. (17 July 2023)
- Information without being screened or analyzed would not enable a third party to gain a competitive advantage upon obtaining it and therefore does not possess economic value. (14 December 2023)

Reasonable Secrecy Measures

- Use of personal email and cloud services by employees without explicit prohibition meant no reasonable confidentiality measures. (19 April 2023)
- Technical drawings were protected despite the public display of machinery's exterior and operation because there were no machine design drawings or dimension data disclosed. (30 June 2023)
- Installation of monitoring software to record employees' actions alone was deemed insufficient to meet secrecy obligations. (19 November 2023)
- Lack of access control mechanisms for electronic files by rank resulted in the finding of insufficient confidentiality measures. (26 November 2023)
- Despite some physical access controls, failure to manage digital dispute-related files led to the denial of sufficient protection. (29 December 2023)

Tort and Civil Damages

- The courts interpreted Article 13(1) to mean that trade secret holders must demonstrate actual impairment of interests or the profits obtained by the misappropriatorer through the act of misappropriation. (7 February 2023)

Criminal Sanctions

- Article 13-1(1), item 2: Unauthorized disclosure beyond permitted use after acquiring trade secrets was found to be criminal. (22 March 2023)
- Article 13-1(1), item 2: Use or disclosure of trade secrets with knowledge of their confidential nature was punishable. (14 April 2023)
- Article 13-1(1), item 1: Determination of Trade Secret Misappropriation through Deception and Improper Means. (16 May 2023)
- A corporation was found not liable where it had taken sufficient preventive measures to prevent its employees from disclosing or using another person's trade secrets. (26 June 2023)

- Article 13-1(1), item 2: Reproduction of trade secrets beyond the approved scope constituted criminal infringement. (8 August 2023)

Protective Orders

- A corporation could not be subject to a confidentiality preservation order because it had no access to the relevant documents or files. (1 February 2023)

Restrictions on Marking or Access

- The confidentiality preservation order and the limited file access regime are recognized as distinct legal means of protection. (27 October 2023)
- The relationship between confidentiality preservation orders and restricted access to litigation materials was further clarified. (18 December 2023)

(19) Thailand

1) Legal Framework and Recent Developments

Thailand protects trade secrets under *the Trade Secrets Act (No.2) B.E. 2558 (2015)*.[106] The Act defines trade secrets as business information that is not publicly known or readily accessible by persons associated with such information, and whose commercial value derives from its secrecy. To be considered a trade secret, the owner must have taken appropriate measures to maintain its confidentiality. In this regard, companies must implement such measures, which may include internal company rules, such as work regulations. Furthermore, information management systems, including internal training and audits, should be established to ensure continued protection.[107]

"Business information" under the Act refers to any form of statement, fact, or medium that conveys meaning—regardless of the method or form of expression. This includes formulas, patterns, compilations, programs, methods, techniques, or processes. A trade secret owner is defined as any person who discovers, invents, compiles, or creates such business information without infringing on others' trade secrets or violating rights of lawful holders, as well as any person lawfully receiving the information.[108]

Trade secret owners may disclose, withhold, use, or authorize others to use the trade secrets.[109]

Misappropriation occurs when a trade secret is disclosed, deprived, or used without the owner's consent and in a manner contrary to honest commercial practices. Such acts are only deemed unlawful if the infringer knew or should have reasonably known the act was dishonest. Acts contrary to honest commercial practice include breach of contract, inducement to breach, breach of confidence, bribery, coercion, fraud, theft, receipt of stolen property, or unauthorized acquisition through electronic or other improper means.[110]

However, the Act provides for specific exceptions to liability. These include:

- acquisition without knowledge that the trade secret was obtained through improper means;
- disclosure by public authorities for reasons of public health or safety;
- independent discovery or development by a researcher; and
- reverse engineering conducted through lawful means.[111]

106 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 3. For the original text of Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, please refer to the following website: https://www.wipo.int/wipolex/en/legislation/details/15720 (last visit on 14 July 2025).

107 Shota Watanabe et al., "Current Status of ASEAN Data Governance and Its Implications for the Digital Economy Framework Agreement", ERIA Discussion Paper Series, No.539 (2025), ERIA-DP-2024-32, p.7.

108 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 3.

109 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 5.

110 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 6.

111 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 7.

2) Civil Remedies

Where there is clear evidence of trade secret misappropriation, the trade secret owner may apply to the court for a preliminary injunction to stop the misappropriation, and may also request a permanent injunction along with a claim for damages.[112]

A civil action for trade secret misappropriation must be brought within three years from the date the owner became aware of the misappropriation and the identity of the infringer, and in any case, no later than ten years from the date of the misappropriation.[113]

In a civil lawsuit, if the owner proves that the defendant's manufactured product is identical to a product that would have been produced using the owner's trade secret, and the defendant fails to present counter-evidence, the court shall presume that misappropriation has occurred.[114]

When assessing damages in a civil action, the court may include both the actual loss incurred by the plaintiff and any profits derived by the defendant from the misappropriation. Furthermore, if there is clear evidence that the misappropriation was committed wilfully or with malicious intent to compromise confidentiality, the court may grant punitive damages in addition to compensatory damages, provided that the punitive damages do not exceed twice the amount of compensatory damages.[115]

3) Criminal Remedies

The Act also provides criminal penalties in certain cases. Obstructing the duties of a trade secret official may result in up to one year of imprisonment, or a fine not exceeding THB 20,000, or both. Failure to cooperate with trade secret authorities may result in up to one month's imprisonment or a fine not exceeding THB 2,000.[116]

If a person discloses or uses a trade secret through media such as documents, audio, or video broadcasts with malicious intent to harm another's business, penalties include up to two years of imprisonment or a fine up to THB 200,000 or both.[117]

Disclosing trade secrets obtained through official duties—whether during public service, investigations, or litigation—may result in up to one year of imprisonment or a fine up to THB 100,000 or both.[118]

112 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 8.

113 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 10.

114 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 12.

115 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 13.

116 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 31 and 32.

117 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 34.

118 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 35.

4) Economy-Specific Features

Thailand has established a Trade Secrets Board to advise on policy, issue recommendations, and assist with mediation or arbitration in disputes.[119] The board is chaired by the Deputy Minister of Commerce, with the Director-General of the Department of Intellectual Property (DIP) serving as vice-chair, and includes senior officials from related ministries and experts from the private sector.[120]

For products such as pharmaceuticals or agrochemicals involving new chemical substances, applicants for regulatory approval must submit supporting information. If such data qualifies as a trade secret—e.g., test results or confidential R&D materials—the competent authority must protect it from unfair commercial use or disclosure, in accordance with regulations issued by the Minister.[121]

5) Cases and Precedents[122]

Thailand has seen increasing trade secret disputes, especially among SMEs investing in R&D for product design, process innovation, and cost reduction. Many such disputes involve current or former employees or business partners, though relatively few result in legal enforcement.

According to the Central Intellectual Property and International Trade Court (IP&IT Court), only 66 trade secret cases were filed between 2004 and 2014. Many were dismissed due to the plaintiff's failure to demonstrate that adequate protective measures had been taken or to identify the confidential nature of the information.

In Supreme Court *Decision No.10217/2553*, the court rejected a claim based solely on general confidentiality and non-compete clauses in an employment contract, holding that such provisions alone did not suffice to demonstrate the existence of trade secret protection. The ruling emphasized the need to clearly identify the protected documents or data and to prove that actual confidentiality measures were in place.

Generally, Thai courts require three elements to establish legal protection for trade secrets:

(a) The information must not be publicly known;

(b) The information must have commercial value;

(c) Reasonable confidentiality measures must have been implemented and must be demonstrable.

Failure to meet any of these elements may defeat a trade secret claim. However, where plaintiffs have demonstrated robust protective measures, there are cases in which Thai courts have rendered favourable decisions, including awards of damages.

As these cases demonstrate, the outcome of trade secret litigation often hinges on whether the company has implemented adequate preventive and security measures. Even outside the courtroom, trade secrets, once leaked, are nearly impossible to recover—making preemptive management and prevention the most critical components of effective protection.

---

119 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 21.

120 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 16.

121 Thailand's *Trade Secrets Act (No.2) B.E.2558 (2015)*, Article 15.

122 European Commission, IP Helpdesk, 'Case Study 28 - Trade Secrets protection in Thailand', https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/south-east-asia-ip-sme-helpdesk/case-studies/case-study-28-trade-secrets-protection-thailand_en (last visit on 14 July 2025).

In practice, employees may not fully recognize the importance of the information they handle. Therefore, regular internal training and clear operational guidelines are essential. Confidentiality markings, access controls, and secure storage protocols must be systematically applied to both electronic and physical documents. It is also important that all employees sign employment contracts containing specific and enforceable confidentiality clauses, with the scope of protected information clearly defined. Such measures must not remain merely on paper, but be effectively implemented and monitored. For small and medium-sized enterprises (SMEs) operating in Thailand, seeking guidance from professionals who are well-versed in local legal and judicial frameworks can be a crucial strategy for ensuring successful trade secret protection.

(20) United States

1) Legal Framework

In United States, trade secrets are protected under both federal and state law. At the federal level, *the Defend Trade Secrets Act (DTSA)* governs civil trade secret misappropriation, while the *Economic Espionage Act (EEA)* criminalizes theft of trade secrets in certain circumstances. In addition, most states of United States have enacted their own trade secret statutes modelled on *the Uniform Trade Secrets Act (UTSA)*, with New York being the only state that has not adopted the UTSA, although it remains subject to federal protection under the DTSA. Other relevant federal statutes include *the Computer Fraud and Abuse Act (CFAA)* and *the Economic Espionage Act (EEA)*, which also provide protections in the context of trade secrets..

The definition of a trade secret varies slightly depending on the applicable legal framework:

- Under the EEA and DTSA, a trade secret is defined as all forms and types of financial, business, scientific, technical, economic, or engineering information—whether tangible or intangible, and regardless of how it is stored, compiled, or memorialized—including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, provided that: (1) the owner has taken reasonable measures to keep such information secret; and (2) the information derives independent economic value, actual or potential, from not being generally known to, or readily ascertainable through proper means by, another person who can obtain economic value from its disclosure or use.
- Under the UTSA, a trade secret is defined as information—including a formula, pattern, compilation, program, device, method, technique, or process—that (1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Under the DTSA and UTSA, the "misappropriation" of trade secrets generally falls into the following two categories:

(a) acquisition of a trade secret by improper means; or

(b) disclosure or use of a trade secret without consent by person who (1) acquired the trade secret by improper means, or (2) knew or had reason to know that trade secret was (i) derived from a person who acquired it by improper means, (ii) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use, or (iii) derived from a person who owed a duty to maintain its secrecy or limit its use.

Improper means include theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. Reverse engineering and independent development are not considered improper means.

In United States, some states recognize the Inevitable Disclosure Doctrine (IDD) as a legal principle in interpreting trade secret misappropriation. The IDD allows employers to seek injunctions against former employees working for competitors, even in the absence of a non-compete agreement or direct evidence of wrongdoing. Courts in jurisdictions recognizing the IDD assess several factors for injunctive relief, including: (1) the degree of competition between employers, (2) similarity between the employee's former and new roles, and (3) the trade secret's value to both employers.[123]

2) Civil Remedies

The DTSA provides for various civil remedies in cases of trade secret misappropriation, including injunctive relief, civil seizure, and monetary damages.

Injunctive relief may be granted to prevent actual or threatened misappropriation. Under the DTSA, an injunction cannot conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade, or business. An injunction also cannot prevent a person from entering into an employment relationship, but can place conditions on such employment based on evidence of threatened misappropriation and not merely on the information the individual knows.

The DTSA also authorizes ex parte civil seizure, which allows property necessary to prevent the propagation or dissemination of a trade secret to be seized without prior notice to the defendant in exceptional circumstances. (See 18 U.S.C. §1836(b)(2)(A)(i)).

This remedy is available where, for example, the defendant is likely to flee United States, imminently disclose the trade secret to third parties, or otherwise frustrate enforcement, such as through destruction or concealment of evidence or deceptive/evasive actions. Recognizing that ordinary injunctions may be insufficient in such cases, Congress included this provision to provide emergency relief.

Civil seizure may be granted if the applicant can demonstrate that immediate and irreparable harm would occur without the seizure, and that the harm to the applicant outweighs the potential harm to the defendant, along with satisfying additional statutory requirements.

In addition to injunctive relief, the DTSA allows for monetary damages for actual loss caused by the misappropriation of a trade secret. The law also permits damages for any unjust enrichment not otherwise accounted for in the calculation of actual damages. In lieu of actual loss and unjust enrichment, the award may constitute damages caused by the misappropriation measured by imposition of liability for a reasonable royalty.

Where willful and malicious misappropriation is established, the DTSA permits exemplary damages of up to two times the amount of actual damages.

123 Andrew Yizhou Liu, "Trade Secrets Protection and Employment of Public Firms: Evidence from the Uniform Trade Secrets Act", Research Policy, Vol.54, No.6 (July 2025), p.2. Please refer to the following website for the original text of the article: https://doi.org/10.1016/j.respol.2025.105243 (last visit on 20 July 2025).

Misappropriation of a trade secret can also serve as the basis for a complaint filed with United States International Trade Commission alleging that importation of certain articles results in misappropriation of a trade secret and constitutes an unfair method of competition. 19 U.S.C. § 1337(a)(1)(A). Following an investigation and determination by the Commission that imported articles misappropriate a trade secret and constitute an unfair method of competition, the Commission may issue an order directing United States Customs and Border Protection to exclude the subject articles from entry into United States. 19 U.S.C. § 1337(d). The Commission may also issue an order directing United States Customs and Border Protection to seize and forfeit the subject articles if the exclusion order is repeatedly violated by a party. 19 U.S.C. § 1337(i).

3) Criminal Remedies

In United States, criminal liability for trade secret misappropriation is primarily governed by *the Economic Espionage Act (EEA)*. The EEA was enacted to combat the theft of trade secrets, including in the context of state-sponsored industrial espionage, and to protect businesses and security interests of United States.

Under the EEA (18 U.S.C. §1831), criminal liability arises where trade secrets are misappropriated with the intent or knowledge that the offense will benefit a foreign government, instrumentality, or agent. The statute prohibits a wide range of unauthorized activities, including the theft, copying, transmission, alteration, destruction, or delivery of trade secrets, whether physically or electronically, as well as attempts or conspiracies to engage in such conduct. Individuals found guilty of violating this statute may face criminal penalties of up to 15 years' imprisonment and fines of up to USD 5 million.

For organizations that commit such an offense, a fine of up to USD 10 million or three times the value of the stolen trade secret, whichever is greater, may be imposed.

Criminal liability under the EEA (18 U.S.C. §1832) also arises with respect to misappropriation of a trade secret related to product or service used in interstate or foreign commerce, for the benefit of anyone other than the owner and intending or knowing that the owner will be injured. Individuals may face up to 10 years of imprisonment or fines, while organizations may be fined up to USD 5 million or three times the value of the stolen trade secret, whichever is greater.

Whereas Section 1831 of *the Economic Espionage Act* targets conduct intended to benefit foreign interests, Section 1832 addresses trade secret theft committed for commercial advantage or economic gain of anyone other than the owner of the trade secret.

4) Economy-specific Features

The Computer Fraud and Abuse Act (CFAA) is a federal statute that imposes criminal and civil liability on individuals who intentionally access a protected computer system without authorization or who exceed authorized access, including when such access results in damage or the acquisition of protected information. This includes, for example, unauthorized access to financial records of a financial institution, information held by a department or agency of United States, or information stored on a protected computer.

In *Van Buren v. United States*, the Supreme Court of United States clarified that the CFAA covers individuals who "exceed authorized access" by accessing a computer with authorization but then obtain information located in particular areas of the computer—such as files, folders, or databases—that are off-limits to them. It does not cover those who have improper motives for obtaining information that they are otherwise authorized to access.

5) Cases and Precedents

Remote work and the increase in conducting internal business through communications platforms rather than in person presents additional challenges for trade secret owners in ensuring adequate and effective measures to preserve secrecy. One state court example is *Smash Franchise Partners, LLC v. Kanda Holdings, Inc.*, decided by the Delaware Court of Chancery on 13 August 2020. The court held that trade secret protection may be compromised if a company fails to implement available security measures when exchanging confidential information online.

In this case, the plaintiff failed to use built-in security features of a web-based videoconferencing platform—Zoom—to protect sensitive business discussions. As a result, the court determined that the information disclosed during public Zoom calls, including confidential and proprietary business strategies, did not qualify for trade secret protection. The ruling emphasized that the plaintiff had not taken "reasonable measures" to preserve confidentiality, as required under the DTSA.[124]

124 Jeong Kwan-Young et al., *supra note 41*, p.55.

(21) Viet Nam

1) Legal Framework

The protection of trade secrets in Viet Nam is primarily governed by *the Law on Intellectual Property of the Socialist Republic of Viet Nam*.[125] Under this law, a trade secret is defined as information obtained from financial or intellectual investment activities that has not been disclosed and is capable of being used in business.[126] The industrial property rights related to trade secrets are established based on the lawful acquisition and maintenance of confidentiality.[127]

To qualify for protection as a trade secret, the information must meet the following criteria:[128]

(a) it must not be common knowledge or readily accessible;

(b) it must confer a competitive advantage to the holder when used in the course of business, compared to those who do not possess or use the information; and

(c) the owner must have taken necessary measures to keep the information confidential and prevent easy access or disclosure.

The use of a trade secret includes:[129]

(a) applying the trade secret in the manufacture of goods, provision of services, or commercial transactions; and

(b) importing, advertising for sale, or storing for sale goods produced using the trade secret.

However, personal secrets, public administrative secrets, public defense or security secrets, and other information unrelated to business activities are not eligible for protection as trade secrets.[130]

A trade secret owner is defined as an organization or individual who lawfully acquires and maintains the secrecy of the information. Unless otherwise agreed between the parties, trade secrets developed by employees or contractors in the course of performing assigned tasks or duties shall belong to the employer or commissioning party.[131]

The following acts are considered infringements of trade secrets:[132]

(a) accessing or acquiring trade secret-related information by breaching confidentiality measures adopted by the lawful manager of the trade secret;

(b) disclosing or using trade secret-related information without the consent of the trade secret owner;

---

125 Viet Nam *Intellectual Property Law (No.50/2005/QH11)*. For the original text of Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, please refer to the following website: https://vietanlaw.com/vietnam-intellectual-property-no-50-2005-qh11/ (last visit on 14 July 2025).

126 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 4.

127 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 6.

128 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 84.

129 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 124.

130 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 85.

131 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 121(3).

132 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 127.

(c) violating confidentiality agreements, or deceiving, inducing, bribing, coercing, tempting, or abusing trust to access, acquire, or disclose trade secrets;

(d) accessing or acquiring trade secret-related information from regulatory agencies by circumventing confidentiality measures during the licensing or approval of goods and services;

(e) using or disclosing trade secrets despite knowing or having a duty to know that they were acquired through infringing acts stipulated by law;

(f) failing to fulfil confidentiality obligations as prescribed by law.

2) Civil Remedies

In Viet Nam, trade secrets are recognized as a form of intellectual property, and therefore, civil, administrative, and criminal remedies under the Law on Intellectual Property are applicable in the event of misappropriation.

Holders of intellectual property rights, including trade secrets, are entitled to:[133]

- adopt technical measures to prevent infringement;
- request the infringer to cease the infringing act, provide a public apology, and pay compensation for damages;
- request competent authorities to take action against acts of infringement; and
- file a lawsuit with the court to protect their legal rights and interests.

Available civil remedies include a court-ordered cessation of infringement, mandatory public apology, enforcement of civil obligations, and compensation for damages.[134]

Damages may cover both material (economic) loss and non-material (emotional or reputational) harm. The level of compensation is to be calculated based on the actual loss suffered by the right holder.[135]

If the plaintiff proves that the infringement resulted in actual physical or economic harm, the court is authorized to determine the compensation amount accordingly.[136]

3) Criminal Remedies

Under *the Criminal Code of Viet Nam*, individuals may be held criminally liable if their infringement of intellectual property rights constitutes a criminal offense.[137]

133 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 198.

134 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 202.

135 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 204.

136 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 205.

137 Viet Nam *Intellectual Property Law (No. 50/2005/QH11)*, Article 212.

While *the Criminal Code*[138] does not explicitly mention "trade secrets," several provisions provide relevant criminal sanctions. Article 159 of *the Criminal Code* criminalizes the infringement of secrecy related to information, mail, telephone, and telegraph communications. This provision penalizes unauthorized access to another person's means of communication, as well as the unlawful collection or disclosure of confidential information. It covers acts such as the illicit acquisition, intentional destruction, or concealment of mail, telegrams, faxes, or other documents; illegal eavesdropping or recording; and the search or seizure of documents without proper authority.

Offenders may be subject to fines or community service. In more serious cases—such as when the act is committed in an organized manner, involves abuse of authority, is repeated, or causes reputational harm to the victim through the disclosure of the obtained information—imprisonment may be imposed. The provision also allows for disqualification from holding a professional position, indicating that sanctions may be applied to employees or executives who misuse their corporate role to disclose confidential information.

Article 288 of *the Criminal Code*, addresses offenses involving the illegal provision or use of information via computer or telecommunications networks. This includes unauthorized publication, sale, or disclosure of personal or confidential data and is particularly relevant to the digital misappropriation of trade secrets. If such acts cause property damage or reputational harm, or result in illegal profits, the offender may be subject to fines, imprisonment, or community service. Aggravating factors include abuse of position, large-scale operations, or significant societal impact.

Article 289 of *the Criminal Code,* criminalizes unauthorized access to another person's computer network or device, including hacking, exploiting administrator privileges, and manipulating or stealing digital data. It provides a legal basis to sanction cyber-theft or destruction of trade secrets. Severe penalties are imposed in cases involving public security, critical infrastructure systems, or high-value data breaches. Collectively, these provisions offer a robust framework for addressing cyber-enabled trade secret misappropriation, which is increasingly common in modern business environments.

4) Economy-Specific Features

In Viet Nam, the terminology used to refer to trade secrets appears to vary across different legal instruments, and in some cases, definitions are imprecise or seemingly inconsistent depending on the applicable statute.

The term "trade secret" appears in several key legislations:

- ***Law on Intellectual Property (No.50/2005/QH11), Article 4:***

  "A trade secret means information obtained from activities of financial and/or intellectual investment, which has not yet been disclosed and can be used in business."

- ***Law on Competition (No. 23/2018/QH14), Article 45:***

  "Trade secret infringement includes: (a) Accessing and acquiring trade secrets by going against security measures of the owner; (b) Disclosing or using trade secrets without the owner's consent."

138 Viet Nam *Criminal Code (No.100/2015/QH13)*. For the original text of Viet Nam *Criminal Code (No.100/2015/QH13)*, please refer to the following website: https://vietanlaw.com/12-2017-qh14-364731/ (last visit on 14 July 2025).

- ***Law on Enterprises (No. 59/2020/QH14), Article 115(2):***

  "Access, extract the minutes of meetings, resolutions and decisions of the Board of Directors, mid-year and annual financial statements, reports of the Board of Controllers, contracts and transactions subject to approval by the Board of Directors and other documents, except those that involve the company's business secrets."

While the concept of "trade secret" is formally defined under the IP and Competition laws, the Enterprise Law refers instead to "business secrets" without providing a statutory definition. The legislative intent behind the Enterprise Law appears to be the protection of sensitive corporate information; however, the lack of definitional clarity and overlap among the terms used in different statutes may give rise to legal uncertainty and create challenges for corporate compliance and transparency.

In practice, the term "trade secret" tends to relate to market transactions, competitive strategies, and external dealings, while "business secrets" typically refer to internal corporate information such as management, production, financial data, and strategic planning. Although a functional distinction may exist, the current legal ambiguity underscores the need for clear definitions and consistent interpretation to avoid confusion and ensure enforceability.

5) Cases and Precedents[139]

Two notable cases in Viet Nam illustrate the economy's evolving judicial approach to trade secrets:

- *Case No.20/LD-ST (17 March 2005)* involved an employee of a company based in United States who emailed product-related information to her sister. The court found that this act violated the company's internal confidentiality regulations, which had been properly established and registered with the labour authority. The court upheld the company's decision to terminate the employee, affirming that disciplinary actions based on legally established and published internal rules are valid and enforceable. This case highlights the Vietnamese judiciary's willingness to recognize corporate internal regulations as a legitimate basis for disciplinary action when they meet legal formalities.
- *Case No.09/2010/LD-ST (10 December 2010)* concerned a former employee who violated a non-compete agreement. Although the agreement did not provide financial compensation and allowed the employer to unilaterally amend the list of competing firms, the court nonetheless upheld its validity. The court viewed the agreement as a civil contract entered into voluntarily by both parties and thus legally binding. This decision reflects a relatively flexible judicial stance toward non-compete clauses in Viet Nam at the time.

139 Loc Xuan Le, "Viet Nam: Protecting Trade Secrets", Tilleke & Gibbins (May 2016). For the original text of this article, please refer to the following website: https://www.tilleke.com/insights/vietnam-protecting-trade-secrets/6/ (last visit on 14 July 2025).

4. Business Support Programs for Trade Secret Protection

Importance of Trade Secrets and the Institutional Landscape in the APEC

- Despite being a core asset underpinning corporate activities—from innovation competitiveness and technological accumulation to market-entry protection—trade secrets are not governed by a common or harmonized legal framework across the APEC
- Some economies maintain standalone trade secret laws or specific legislative provisions, while others rely on general legal principles such as non-disclosure agreements (NDAs), common law doctrines, or contract law to protect trade secrets.
- Although terminology varies across economies—trade secret, business secret, commercial confidential information, corporate secrecy—the underlying nature of trade secrets as critical information for business competitiveness remains consistent, and their importance continues to grow.
- However, significant institutional disparities among APEC economies result in uneven foundations for SMEs to manage and protect trade secrets effectively, with capacities differing substantially by jurisdiction.

Need for Business Support Programs for Trade Secret Protection

- With rising risks such as technology leakage, employee mobility, and increasing vulnerabilities in supply chains, the need for trade secret protection support for SMEs has grown significantly. SMEs, in particular, tend to have markedly weaker capabilities and awareness in managing trade secrets compared to large enterprises, due to the absence of dedicated security teams, insufficient internal policies, and limited access to legal and regulatory resources.
- In response, some economies have introduced programs specifically aimed at supporting enterprises in protecting trade secrets; however, programs designed exclusively for trade secret protection remain very limited.
- By contrast, a larger number of economies operate broad-based SME support programs, some of which incorporate intellectual property protection, information security, and digital security as key components, thereby including trade secret protection indirectly as part of their overall support measures.

Business Support Programs for Trade Secret Protection

- The following section presents cases from APEC member economies that operate dedicated platforms, policy tools, or institutional programs specifically aimed at supporting trade secret protection
- These examples provide insights for the future introduction or enhancement of trade secret protection programs tailored to the needs of SMEs.

(1) Selected Support Programs in People's Republic of China

National Innovative Pilot Program for Trade Secret Protection by the State Administration for Market Regulation (SAMR)[140]

- On 2 March 2022, the State Administration for Market Regulation (SAMR) announced the 'National Innovative Pilot Program for Trade Secret Protection.' The objectives are to strengthen trade secrets protection, enhance the fight against unfair competition, improve firms' creative capacity and market dynamism—thereby contributing to high-quality economic development.
- The program designates selected regions as pilot zones, where institutional approaches and protection models can be tested before being scaled up nationwide. Through this process, the program also aims to elevate the level of internationalization in People's of Republic of China's trade secret protection system and enhance its responsiveness to evolving global trade conditions.
- During the pilot period, the program seeks to: (i) strengthen institutional innovation in trade secret protection; (ii) build and refine working mechanisms for trade secret protection; (iii) strengthen regulatory law enforcement for trade secret protection; (iv) improve the service and support system for trade secret protection; (v) align with high-standard international economic and trade rules, etc.
- Based on this national initiative, individual municipalities have developed and implemented their own specialized local plans tailored to their regional conditions.

Trade Secret Protection Support Program of Minhang District, Shanghai [141]

- In alignment with SAMR's National Innovative Pilot Program, Minhang District of Shanghai announced its implementation plan for a three-year pilot initiative (2025–2027), which includes several measures specifically tailored to the needs of SMEs.
- **Enterprise-level protection measures:** The plan identifies technology-intensive, new-technology, innovation-driven, and knowledge-intensive enterprises as priority beneficiaries, with particular emphasis on firms operating in high-end sectors such as biopharmaceuticals, artificial intelligence, next-generation information technology, and advanced equipment manufacturing.
- **Provision of specialized services:** Tailored services are offered to enterprises—including SMEs—such as employee confidentiality training, trade secret evidence preservation, forensic analysis of electronic data, investigation and evidence collection, and loss assessment.
- **Establishment of pilot units within industrial parks:** The district promotes the creation of trade secret protection pilot units across industrial parks, enabling the development and testing of applicable protection models for enterprises located in these clusters.

140 State Administration for Market Regulation, "Notice on Printing and Distributing the Work Plan for the National Innovation Pilot for Trade Secret Protection" (2 March 2022). For the original text of this document, please refer to the following website: https://www.gov.cn/zhengce/zhengceku/2022-03/23/content_5680784.htm (last visit on 24 November 2025).
141 Minhang District People's Government, "Notice of Issuance of the Implementation Plan for Minhang District to Advance the National Trade Secret Protection Innovation Pilot (2025-2027)" (24 October 2025). For the original text of this document, please refer to the following website: https://www.shanghai.gov.cn/gwk/search/content/deb01b7c2d6b494396d5bf6a66e9a7b5 (last visit on 24 November 2025).

- **Enhanced awareness-raising and training for enterprises:** Programs include cultivating professional talent for trade secret protection, conducting outreach seminars, and delivering training—particularly for SMEs and startups located within industrial parks and business associations.
- **Enterprise consultation and support networks:** Industrial parks host consultation and assistance centers that help identify enterprise-level issues, provide advisory services, and support problem-solving, thereby improving SMEs' access to trade secret protection resources.

Trade Secret Protection Support Program of Shijiazhuang, Hebei[142]

- In conjunction with the AMR's National Innovative Pilot Program, Shijiazhuang City in Hebei Province has incorporated SME-oriented, tailored measures into its implementation plan for the 2025–2027 pilot initiative.
- The plan designates knowledge-intensive, technology-intensive, innovation-driven, and well-established brand enterprises as key protection targets, thereby encompassing SMEs and startups within the broader group of innovative enterprises.

Trade Secret Protection Support Program of Yinchuan[143]

- Aligned with SAMR's National Innovative Pilot Program, Yinchuan City has developed an implementation plan for the 2025–2027 pilot period, aiming to expand the number of trade secret protection bases to at least six and protection stations to more than sixty by the end of 2027. This structure is designed to enhance SMEs' access to trade secret-related consultation and support services within the region.
- The plan also establishes a broad social service network by setting up dedicated trade secret units within public organizations—such as intellectual property service agencies, legal and forensic institutions, industry associations, and universities—to provide enterprises with consultation, training, and coordinated support services.

142 Shijiazhuang Municipal People's Government Office, "Interpretation of the Implementation Plan of Shijiazhuang City to Promote the National Trade Secret Protection Innovation Pilot (2025–2027)" (9 June 2025). For the original text of this document, please refer to the following website: https://www.sjz.gov.cn/columns/5e07049d-1b86-4736-af3d-f62945304c23/202507/18/26b69d2e-bb99-4749-88cf-39984056aaf7.html (last visit on 24 November 2025).
143 Yinchuan Municipal People's Government Office, "Notice on Issuing the 'Implementation Plan for Yinchuan City to Build the National Trade Secret Protection Innovation Pilot (2025-2027)'" (28 February 2025). For the original text of this document, please refer to the following website: https://www.yinchuan.gov.cn/zzb/szfwj/202503/t20250303_4843656.html (last visit on 24 November 2025).

(2) Selected Support Programs in Japan

National Center for Industrial Property Information and Training (INPIT)

- To support the business activities of medium-sized enterprises, SMEs, and startups across Japan, INPIT has established "Comprehensive IP Support Desks" in all 47 prefectures, providing more than 110,000 consultations annually.
- INPIT operates various specialized consultation windows—including Industrial Property Consultation, the Trade Secret Consultation Desk, the Overseas Expansion IP Consultation Desk, the Academia IP Consultation Desk, and the Start-up IP Consultation Desk—to respond to the diverse consultation and support needs of enterprises.

INPIT's Trade Secret Consultation Desk

- INPIT's Trade Secret Consultation Desk provides free-of-charge services to SMEs and other enterprises, including assistance in identifying confidential information—such as technical know-how, product ideas, and customer data—guidance on appropriate management methods, and support for conducting in-house seminars on trade secret protection.
- The desk also offers access to IP Strategy Experts who support enterprises in establishing trade secret management systems, responding to trade secret leakage incidents, strengthening information security measures, and developing IP strategies that integrate rights management with trade secret controls.
- These IP Strategy Experts are highly specialized professionals with advanced expertise and extensive practical experience in IP strategy, gained through direct engagement with enterprises and innovation sites. Their activity areas and profiles are available on the INPIT website: https://www.inpit.go.jp/katsuyo/ip_strategyexp/index.html
- Applications for support may be submitted via telephone, website (noted above), or email, and enterprises can request consultations by providing the necessary information on their specific IP-related needs.
- Support provided by IP Strategy Experts consists of advisory services aimed at helping applicants address their IP-related challenges; however, the experts do not assume responsibility for the outcomes of such advice. Accordingly, they do not participate in activities such as attending licensing or contract negotiations, drafting contracts, preparing filing documents, or performing translation work.

Other Information Related to Trade Secret Protection

- **Ministry of Economy, Trade and Industry (METI)**: METI publishes a wide range of materials related to trade secret protection. These include: pamphlet for employees "Things about Trade Secrets You Should Know About"; Management Guidelines for Trade Secrets; Handbooks for Protection of Confidential Information; Tips for Data Utilization (only available in Japanese); Guidance for Data Utilization; Key Points for Managing Confidential Information during remote work (only available in Japanese).

(3) Selected Support Programs in Republic of Korea

Main Functions of the Trade Secret Protection Center [144]

- **Trade Secret Protection Training**: Provides educational programs and content on trade secret protection systems and management methods to enhance enterprises' capabilities in trade secret management and dispute response.
- **Basic Consulting:** Trade secret experts review a company's current management practices to identify weaknesses in its trade secret protection system and provide guidance for improvement.
- **Advanced Consulting:** Trade secret experts participate directly in the company's internal improvement process, supporting the introduction and enhancement of a tailored trade secret management system that reflects the company's size, industry characteristics, and the nature of confidential information handled.
- **Trade Secret Original Proof (Deposit) Service:** Registers electronic documents containing trade secret information with an authorized deposit institution, enabling companies to verify the existence of the trade secret, the identity of the original holder, and the date of possession in the event of a dispute.
- **Deployment and Operation of Trade Secret Management Systems:** Provides SMEs with access to a trade secret management system that can be implemented using only PC-level computing resources, enabling them to manage their trade secret materials more effectively.
- **Legal Advisory Services for Trade Secret Misappropriation Disputes:** Trade secret–specialized attorneys provide legal advice on whether the Unfair Competition Prevention Act may apply to a trade secret infringement case, suggest potential legal response strategies, and offer guidance on the necessary documentation required for pursuing such claims.

Basic Consulting for Trade Secret Management Systems

- **Content:** Trade secret experts review the company's current management practices, identify weaknesses, and propose feasible trade secret management measures appropriate to the company's capability level.
- **Support Procedure:** Public announcement → Application for consulting → Scheduling consultation → Employee survey & expert assignment → Expert consultation → Request for follow-up measures
- **Eligible Beneficiaries:** Startups, SMEs, universities, and public institutions
- **Support Details:** Provision of an overall assessment grade, review of management practices by category, recommendations for improvement, guidance on phased action items, and follow-up support measures.

Advanced Consulting for Trade Secret Management Systems

- **Content:** Trade secret experts directly participate in the company's internal process to improve its trade secret management system, supporting the introduction and enhancement of a tailored system that reflects the company's size, industry characteristics, and the nature of key confidential information handled.
- **Support Procedure:** Public announcement and application → Evaluation and selection → Final selection of participating companies → Payment of company contribution → Expert matching → On-site consulting → Satisfaction assessment

144 Trade Secret Protection Center, "Official Website of the Trade Secret Protection Center (Republic of Korea)." For more information on this center and its services, please refer to the following website: https://www.tradesecret.or.kr/main.do (last visit on 24 November 2025).

- **Eligible Beneficiaries:** SMEs, medium-sized enterprises, universities, and public research institutes
- **Support Details:** Assessment of the company's current trade secret management system through preliminary surveys, on-site inspections, and interviews based on the standard trade secret management framework; identification of vulnerabilities across management categories; support for improving organizational management practices such as confidentiality classification, review of forms and regulations, and separation and storage of confidential materials; and support for raising internal awareness through employee training and internal declaration events.

Trade Secret Management System

- **Contents:** Provides SMEs with a system that integrates essential functions required for trade secret management, enabling them to manage their trade secret materials effectively using only PC-level computing resources.
- **Support Procedure:** System application → System distribution → System installation
- **Eligible Beneficiaries:** Micro and small enterprises
- **Key Functions:** Management of confidential documents, access control, personnel management, and history/statistics management
- **Expected Benefits:** Cost reduction, demonstrable enhancement of confidentiality management, and increased organizational awareness of trade secrets.

Legal Advisory Services for Trade Secret Misappropriation Disputes

- **Content:** Provides legal consultation by trade secret–specialized attorneys to help enterprises respond effectively at the early stages of a trade secret leakage incident.
- **Support Procedure:** Application submission → Scheduling consultation → Legal consultation → Satisfaction survey
- **Eligible Beneficiaries:** SMEs, universities, public institutions, and prospective entrepreneurs
- **Support Details:** Advice on the feasibility of legal remedies; guidance on relevant laws for effective responses to key legal issues; provision of documentation checklists required for civil and criminal actions; and information on expected litigation costs in trade secret disputes.

Trade Secret Consultation

- **Legal Consultation:** Covers the concept and types of trade secrets, relevant laws and regulations, forms of trade secret misappropriation, preventive measures for trade secret protection, civil and criminal remedies for trade secret infringement, proposed amendments to trade secret legislation, and the trade secret original-proof (deposit) system.
- **Management Consultation:** Covers trade secret management planning, institutional management measures, personnel management measures, physical management measures, monitoring of management practices and corresponding improvement actions, identification of trade secrets, and guidance on the Trade Secret Original Proof (deposit) service and trade secret management systems.

(4) Selected Support Programs in Singapore

Trade Secrets Enterprise Guide in IPOS[145]

- To help businesses and innovators better protect and manage their trade secrets, IPOS published the Trade Secrets Enterprise Guide (2022). The guide includes practical examples of tools and services that enterprises can use to safeguard their trade secrets.
- According to an enterprise survey, 75% of respondents stated that trade secrets are "highly important" to their business, yet half indicated that they lacked adequate understanding of the relevant legal framework. Moreover, 40% reported that they had never used any trade secret–related service.
- Among SMEs, basic protective measures—such as classification of confidential documents, access control, and internal manuals—tend to be weak. Many SMEs also have limited experience in inventorying their confidential assets, resulting in cases where they are unable to identify "what constitutes a trade secret."
- The guide provides practical checklists tailored to SMEs, including essential components of NDAs for employees, physical and technical security checklists, procedures for managing departing employees, and precautions when dealing with third parties. It is designed with SMEs in mind—particularly those without in-house legal teams.
- Beyond the publication of the guide itself, IPOS also delivers enterprise training sessions, co-hosts seminars with partner organizations, offers the "Trade Secret Tool Kit" management platform, and provides guidance on protective measures for companies expanding overseas.

Example of Practical Cases Illustrating the Average Level of Trade Secret Protection in SMEs

- **Case 1: (Cynopsis Solutions – RegTech Company)** An SME that successfully entered overseas markets by obtaining the international security standard certification ISO/IEC 27001:2013, thereby strengthening its credibility and trade secret protection capabilities.
- **Case 2: (Rigel Technology – Smart Sanitary Equipment Manufacturer)** An innovative company specializing in smart sanitary equipment development experienced an incident where a former employee leaked confidential information to a competitor. Following the incident, the company introduced preventive measures such as enhanced access controls for document and email classification, restricted permissions for shared drives, and strengthened NDAs. This case illustrates how SMEs may suffer harm due to weak internal controls and how they subsequently rebuild and improve their internal trade secret management systems.
- **Case 3: (Nutrition Technologies – AgriTech/Biodegradation Technology Company)** A company that manufactures insect-based protein and fertilizer products, which successfully protected and scaled its technologies by adopting the trade secret management platform "Tangibly."

145 Intellectual Property Office of Singapore, "Trade Secrets Enterprise Guide", https://www.ipos.gov.sg/about-ip/trade-secret/ (last visit on 24 November 2025).

(5) Selected Support Programs in Viet Nam[146]

Corporate-Targeted Intellectual Property Management Training & Advisory Program (2024)

- This program was designed to strengthen the intellectual property (IP) management capabilities of Vietnamese enterprises and to help them better protect and utilize their internal assets. Implemented jointly by WIPO and the Intellectual Property Office of Viet Nam (IP Vietnam), the program provides training sessions and advisory services that enable companies to clearly identify their IP assets, establish appropriate management systems, and leverage those assets strategically.
- Recognizing that many enterprises—particularly SMEs and innovative firms—have limited awareness of IP and weak internal management structures, the program offers practical toolkits and mentoring-based support that companies can directly apply to their operational needs.
- **Training Program Delivery:** Training sessions are provided to corporate representatives on subjects such as IP management strategy, asset identification and protection, and technology transfer and commercialization. The curriculum especially includes checklists for identifying and managing IP assets within the company, and guidance on policy drafting and internal governance.
- **Advisory and Mentoring Support:** Analyses are conducted on a company's patent, trademark, and technological or knowledge-based assets, and tailored advisory services are offered to help formulate IP utilization strategies for boosting market competitiveness. The support also includes methods for enterprises with technology or IP bases to reduce the risk of leakage or infringement from external sources.
- **Network and Information Access Enhancement:** Through networks such as TISC (Technology and Innovation Support Center) and IP-Hub, universities, research institutions, and companies are enabled to access IP information and advisory services. The initiative provides pathways for enterprises to connect to technology and innovation data, IP databases, international treaty frameworks, and exchange programmes.

Corporate-Targeted Intellectual Property Management Training & Advisory Program (2025)[147]

- On 21 October 2025, the IP Management Clinic (IPMC) was held in Ho Chi Minh City, Viet Nam, jointly organized by WIPO, IP Vietnam, the WIPO Singapore Office, the ASEAN Business Advisory Council, the ASEAN Secretariat, and WeLead Viet Nam.
- Following the 2024 edition, the 2025 event attracted 80 participating companies, of which 62 were SMEs. Participating firms represented a broad range of technology-intensive sectors, including educational technology, biotechnology, food technology, agricultural technology, information technology, healthcare, and pharmaceuticals.

---

146 Vietnam Intellectual Property Office (IP Vietnam), "WIPO and the National Office of Intellectual Property Launch Training and Consulting Program on IP Management for Vietnamese Enterprises" (29 November 2024). For the original text of this article, please refer to the following website: https://www.ipvietnam.gov.vn/web/guest/hot-news-tisc_ip-hub/-/asset_publisher/OVX2E6EdHTmH/content/to-chuc-so-huu-tri-tue-the-gioi-va-cuc-so-huu-tri-tue-trien-khai-chuong-trinh-ao-tao-va-tu-van-quan-tri-so-huu-tri-tue-cho-doanh-nghiep-viet-nam (last visit on 24 November 2025).

147 World Intellectual Property Organization (WIPO), "Startups and SMEs in Viet Nam Leveraging IP for Innovation and Business Growth through the WIPO Scaled-up IP Management Clinic" (30 October 2025). For the original text of this article, please refer to the following website: https://www.wipo.int/en/web/business/w/news/2025/startups-and-smes-in-viet-nam-leveraging-ip (last visit on 24 November 2025).

- The programme consisted primarily of presentations and discussions focused on guiding enterprises to identify and protect their IP assets and to leverage these assets to enhance brand recognition, attract investment, and generate revenue. In addition, 15 selected companies participated in one-on-one mentoring sessions with business experts, and the organizers announced plans to provide follow-up online advisory services.
- According to participant feedback, the programme enhanced companies' understanding of different IP categories (patents, trademarks, trade secrets, etc.) and strengthened awareness that trade secret management and strategic IP utilization are critical for maintaining competitiveness and supporting business growth.

5. Analysis of Survey from APEC Member Economies

(1) Overview of Responses

A total of 11 APEC member economies submitted responses to the survey questionnaire under the IPEG 102 2024A project. The submissions reflect diverse legal systems, enforcement structures, and levels of digital readiness within the APEC region. Despite this diversity, the survey results show broad convergence in key areas, including:

- Recognition of increasing digital risks to trade secrets;
- Persistent enforcement challenges, especially in evidence collection;
- Strong demand for practical tools for MSMEs; and
- Clear support for APEC-level cooperation and shared resource development.

The following subsections provide a detailed analysis of responses to Questions 1–12.

(2) Q1–Q4: Legal and Enforcement Environment

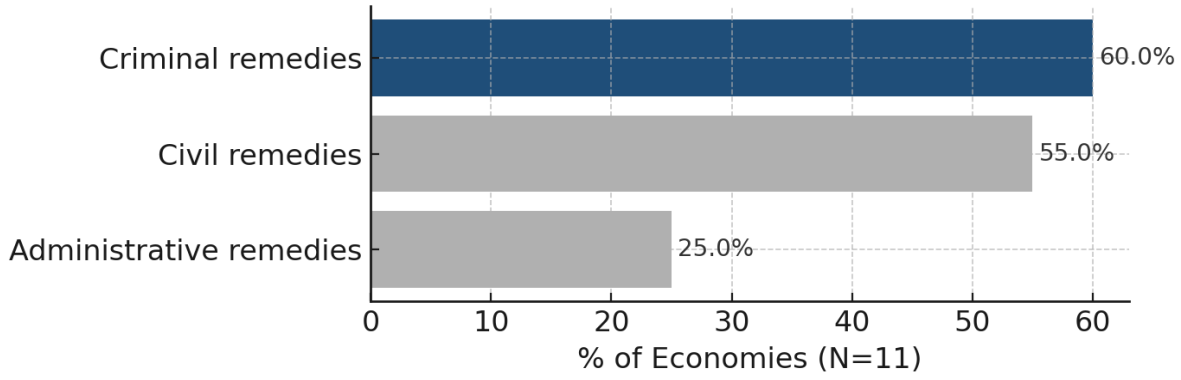
1) Preventive Measures (Q1)

Survey results indicate that contractual measures (e.g., NDAs) are by far the most widely used and most frequently prioritized preventive tool across economies. Based on weighted responses (Peru counted as one economy), approximately 59%of economies selected contractual measures as their primary or most effective approach. This places contractual mechanisms well ahead of other preventive categories.

Technical and physical measures and legal sanctions were also selected by many economies, but they tended to appear as supplementary layers rather than the principal line of defense. The strong preference for contractual safeguards suggests that economies continue to rely most heavily on binding legal commitments and workforce confidentiality obligations as the foundation of trade secret protection.

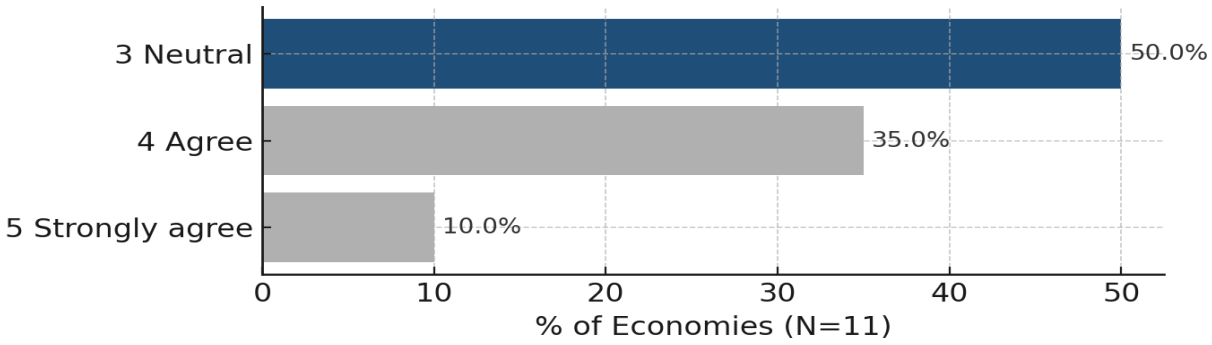
2) Effective Remedies and Deterrence (Q2)

Civil remedies and **criminal sanctions** were widely regarded as critical deterrent tools. This reflects a dual approach where civil remedies address economic restitution, while criminal sanctions provide strong punitive deterrence for serious infringements. Administrative remedies showed greater variation, reflecting different institutional structures among economies. ADR mechanisms were rarely selected, indicating continued reliance on formal adjudicatory systems for trade secret disputes.



3) Effectiveness of Current Enforcement (Q3)

Views on the deterrent effect of punitive damages were divided. Economies that have established punitive damage systems, such as **People's Republic of China** and **United States**, strongly affirmed their effectiveness as a deterrent. However, a significant number of economies (e.g., Hong Kong, China; Mexico; Peru) responded with "Not sure" or "Disagree," largely because such systems are either absent in their jurisdictions or their impact has not yet been empirically observed.



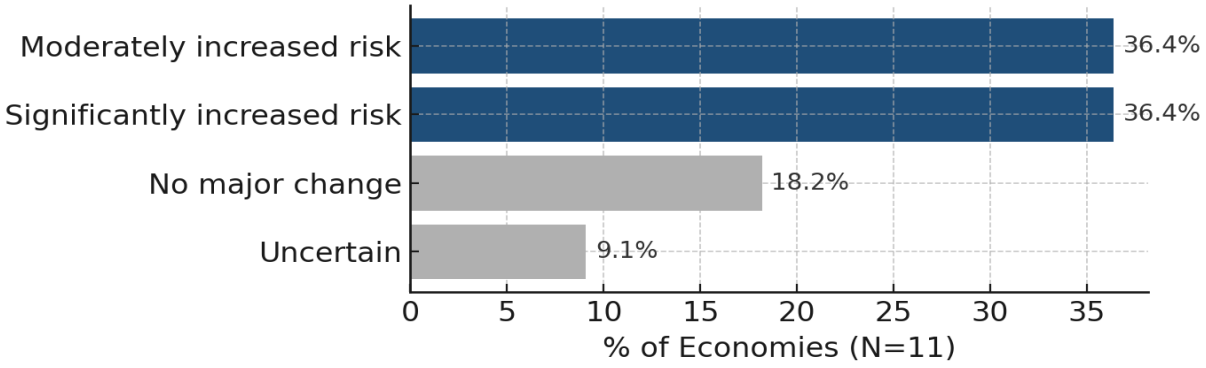
4) Key Enforcement Challenges (Q4)

Proving misappropriation in court was cited as the single most significant challenge by an overwhelming majority of economies (**over 85%**). The burden of proof—specifically regarding the establishment of secrecy and securing admissible evidence—is a nearly universal hurdle, shared by both developed and developing economies (including People's Republic of China; Japan; Republic of Korea; United States). Other challenges, such as lack of awareness (Indonesia; Mexico), were secondary to this systemic procedural barrier.

(3) Q5–Q7: Digitalisation, Remote Work, and AI-Driven Risks

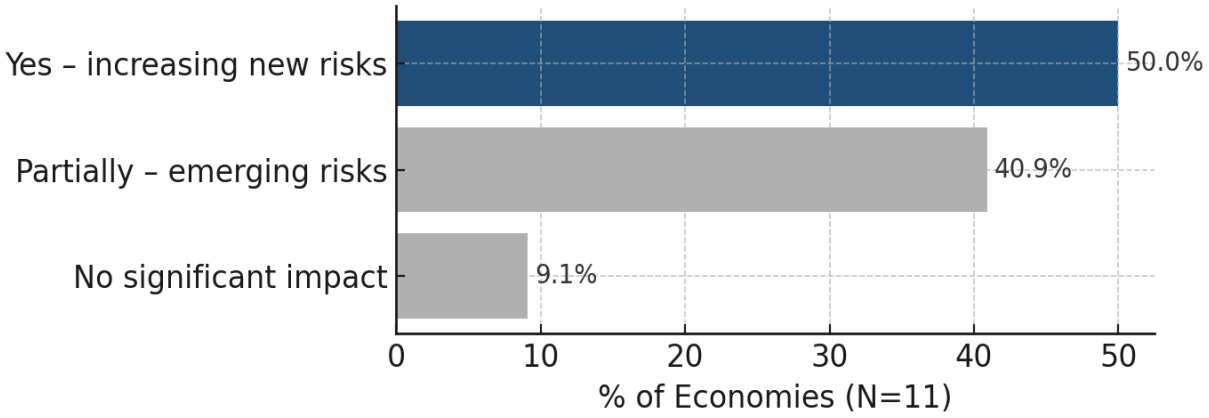
1) Remote Work and Digital Collaboration (Q5)

Most economies reported that digitalization and remote work arrangements have increased trade secret risks. Identified contributors include the expanded use of cloud-sharing systems, remote access environments, and the inherent difficulty of monitoring data flows outside physical office perimeters.



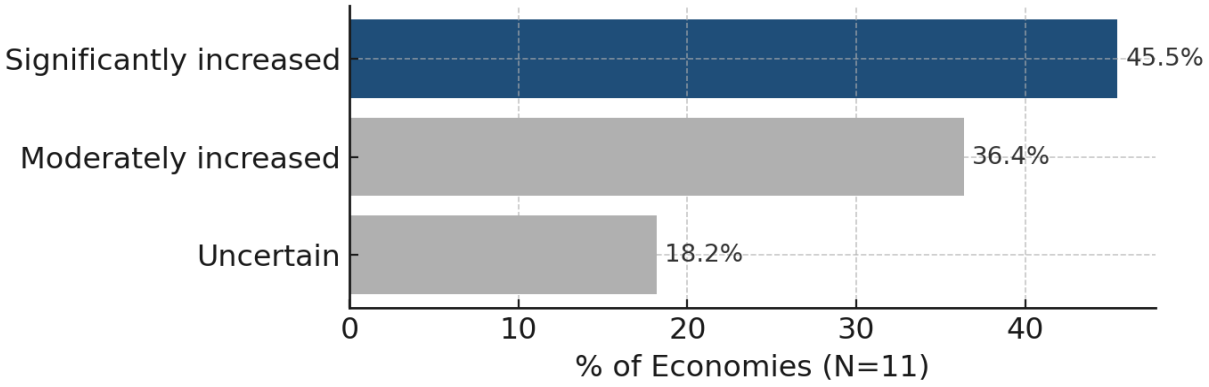
2) AI and Automation Risk Perceptions (Q6)

Responses revealed a **perception gap** regarding AI risks. Tech-intensive economies (e.g., **People's Republic of China; Japan; Republic of Korea; United States**) explicitly identified AI tools as generating "new forms of misappropriation," as experts have described how AI has fundamentally transformed both the methods and scale of trade secret misappropriation. In contrast, several other economies (e.g., **Hong Kong, China; Indonesia; Thailand**) viewed the link as "not yet clear" or merely "potential," suggesting that AI-driven threats have not yet become a mainstream enforcement issue in all jurisdictions.



3) Cyber-based Misappropriation Trends (Q7)

A decisive majority reported that **cyber-based trade secret misappropriation** has significantly increased. Economies noted a shift from physical theft to digital intrusion, cloud compromise, and credential-based attacks. This consensus underscores that trade secret protection is increasingly converging with cybersecurity.

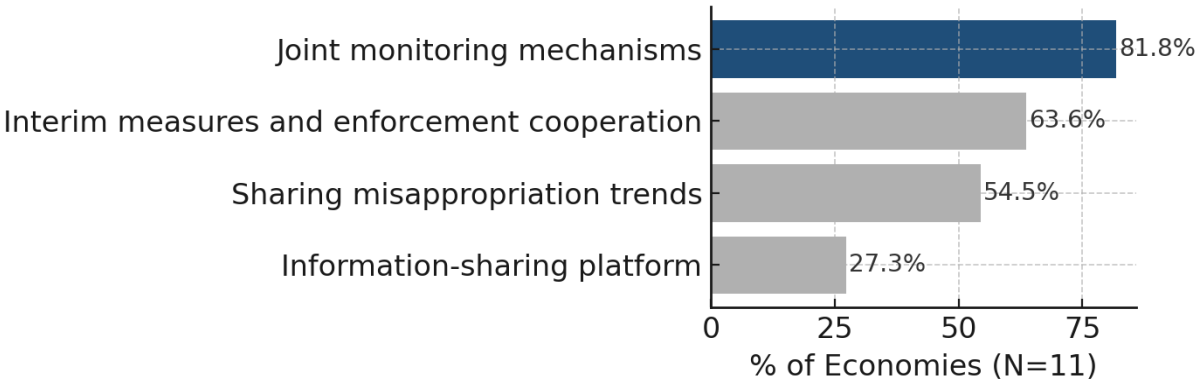


(4) Q8–Q10: MSME Needs and Capacity Building

1) Priority Areas for Regional Cooperation (Q8)

Responses show strong demand for:

- Cross-economy sharing of misappropriation trends;
- Information-sharing mechanisms among platform providers; and
- Strengthening interim measures. These preferences reflect a shared recognition that isolated domestic efforts are insufficient to address cross-border digital infringement.

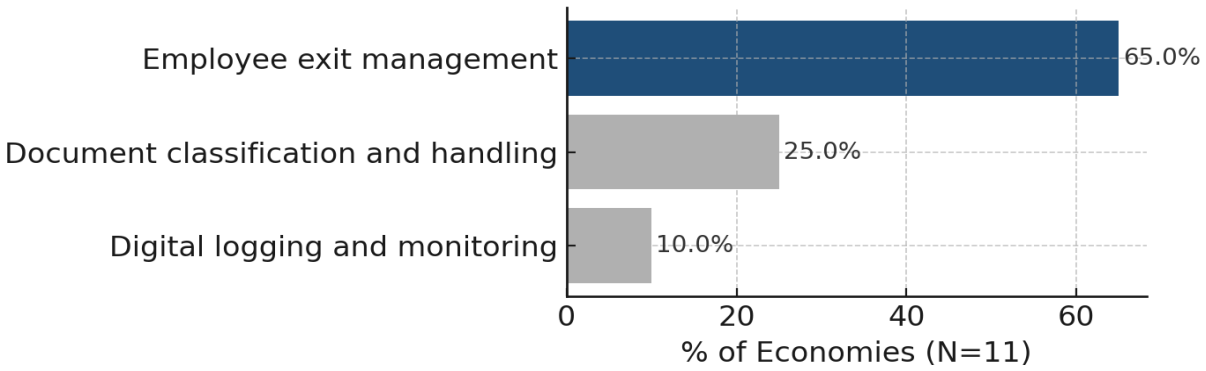


2) MSME Support Tools (Q9)

Economies demonstrated a clear preference for **practical checklists or guidelines**(**54.5%**, including People's Republic of China; Japan; Republic of Korea; United States), followed by **template agreements**(Australia; Hong Kong, China; Thailand). This reinforces the finding that MSMEs require simple, self-assessment tools to lower the barrier to entry for trade secret management.

3) MSME Internal Weaknesses (Q10)

The most frequently cited weakness was **employee exit management**, underscoring the prevalence of insider-related risks. Additional vulnerabilities included document classification, monitoring limitations, and access control for suppliers/partners.

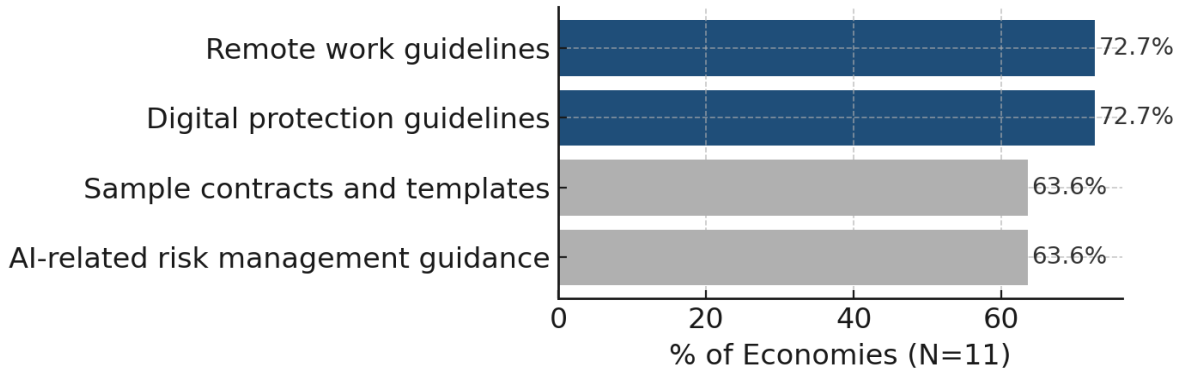


(5) Q11–Q12: Preferred APEC-Level Initiatives

1) Priority Policy Areas (Q11)

Economies expressed strong interest in developing:

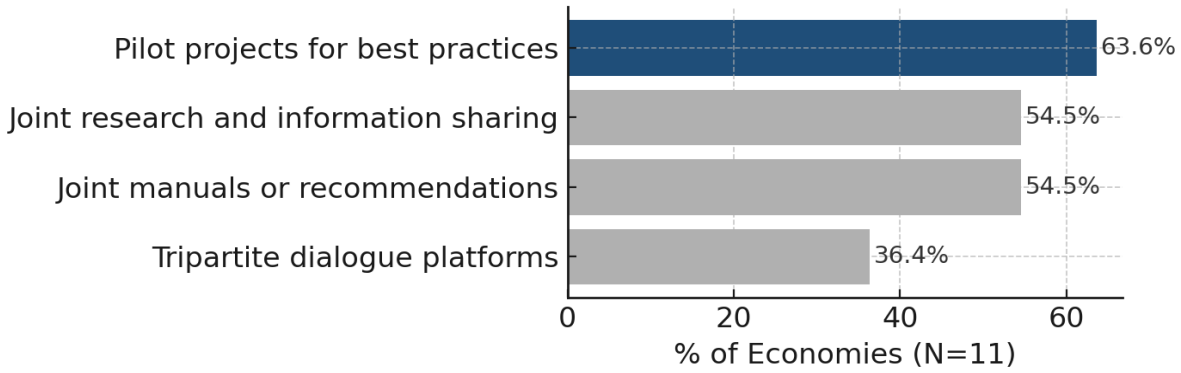
- **Situational checklists** tailored to SMEs;
- Guidance on protecting **AI-generated/related data**; and
- Guidelines for **remote work** environments. These priorities indicate a clear preference for operational, implementation-oriented support that addresses emerging digital realities.



2) Preferred Joint Initiatives (Q12)

The most widely supported initiatives were:

- Pilot projects to identify and share best practices;
- Joint manuals or recommendations; and
- Tripartite dialogue platforms involving government, business, and experts. These areas align with APEC's strengths in consensus-building and practical cooperation rather than formal legislative harmonization.



(6) Key Findings

Based on the analysis of responses, the survey highlights five core findings that define the current landscape of trade secret protection in the APEC region:

1) Digital transformation is fundamentally reshaping trade secret risks.

Across the region, economies consistently observed that digitalization, remote work arrangements, and cloud-based collaboration tools have significantly elevated exposure to trade secret misappropriation. Cyber-based attacks and unauthorized data transfers have rapidly supplanted traditional forms of physical infringement.

2) Enforcement barriers remain systemic and widely shared.

Despite established legal frameworks, enforcement is constrained by structural challenges. The burden of proof—especially proving secrecy and securing digital evidence—was the most frequently cited obstacle (72.7%). This challenge is prevalent across both developed and developing economies.

3) MSMEs face pronounced capability gaps.

MSMEs struggle with limited internal safeguards and low awareness. Economies overwhelmingly indicated that MSMEs need practical, ready-to-use tools—such as checklists and model NDAs—rather than complex legal frameworks. This underscores the need for tailored, resource-efficient support.

4) Economies strongly prefer structured regional information-sharing.

There is clear enthusiasm for cross-economy cooperation, particularly through platforms that facilitate the exchange of misappropriation trends and emerging risk patterns to reduce information asymmetry.

5) APEC members favor action-oriented, practical initiatives over formal harmonization.

Survey responses demonstrate a marked preference for pilot projects, shared manuals, and dialogue platforms. Rather than pursuing legislative harmonization, economies favor flexible, operational initiatives that can be readily implemented and scaled.

(7) Implications for the Practical Guide

The survey findings outlined above provide a clear roadmap for the **"Practical Guide for Safeguarding Trade Secrets."** To effectively address the identified gaps—particularly evidentiary challenges and MSME constraints—the Guide incorporates the following four strategic implications:

1) Strengthening "Evidence Readiness" to Address Enforcement Challenges

With "proving misappropriation" identified as the most significant enforcement barrier (Finding #2), the Guide moves beyond general protection principles to emphasize **"forensic readiness."** It places strong emphasis on identifying, classifying, and documenting trade secrets—foundational steps that enable enterprises to demonstrate "reasonable efforts" in litigation. Accordingly, the Guide integrates protocols for maintaining access logs and preserving digital evidence chains to secure necessary proof before a dispute arises.

2) Delivering "Plug-and-Play" Tools Tailored for MSMEs

Reflecting the specific needs of MSMEs (Finding #3), the Guide is structured as a practical **"Toolkit."** Instead of theoretical legal advice, it features ready-to-use NDAs, self-assessment checklists, and internal policy templates. These tools are designed to be adopted immediately by MSMEs with limited legal or financial resources, allowing them to establish a baseline of protection without incurring significant costs.

3) Managing "Human-Factor" Risks Across the Employment Lifecycle

To mitigate insider threats and clarify exit procedures, the Guide adopts a **lifecycle security approach**. It provides specific guidance covering the entire spectrum of employment—from on boarding confidentiality training and access control during active employment to structured off boarding procedures, such as return-of-assets checklists and exit interviews.

4) Integrating "Digital Safeguards" for the Modern Work Environment

Responding to the reshaping of risks by digital transformation (Finding #1), the Guide integrates essential **technical safeguards**. These include encryption, access control, log management, and digital hygiene practices. By complementing traditional physical controls with digital security measures, the Guide ensures alignment with today’s borderless and technology-driven business environments

6. Conclusion

1) Overview of Project Achievements

The IPEG 102 2024A project, titled “A Practical Guide to Safeguard Trade Secrets for MSMEs in APEC Economies,” was initiated to support the sustainable growth and resilience of Micro, Small, and Medium Enterprises (MSMEs) in the APEC region.

This project conducted a comprehensive comparative review of trade secret legal frameworks across APEC economies together with a survey of 11 member economies to understand the practical challenges faced by MSMEs. The findings show that while member economies have progressively strengthened statutory protections for trade secrets, significant disparities remain in enforcement mechanisms. Concurrently, MSMEs continue to encounter practical difficulties—including digital-era risks, cross-border data exposure, and challenges in substantiating misappropriation in civil proceedings.

Synthesizing these findings, this report concludes that the effectiveness of trade secret protection in the APEC region depends on enhancing the practical capacity of MSMEs to manage, document, and protect their confidential information. Consequently, future cooperation can serve as a catalyst for action-oriented initiatives that equip businesses with tangible tools and management strategies within the existing IPEG framework.

2) Key Insights from the Survey and Legal Analysis

The integration of the survey analysis into this final report has crystallized three strategic insights that drive the proposed way forward:

First, the region is undergoing a clear "Digital Transformation of Risk." Survey responses indicate that remote work, shared workspaces, and cloud-based collaboration have expanded the pathways through which trade secrets may be accessed or leaked (Survey Q5, Q7). Moreover, the emergence of Generative AI has introduced legal ambiguities regarding data ownership and inadvertent disclosures, with advanced economies explicitly identifying AI as a new vector for misappropriation (Survey Q6).

Second, the "Evidentiary Barrier" remains the most significant challenge for enforcement. The survey identified "proving misappropriation in court" as the single most significant challenge, cited by over 85% of respondents (Survey Q4). Many MSMEs struggle to maintain basic internal records—such as access logs or classification notes—that are often needed to demonstrate reasonable secrecy efforts.

Third, there is an overwhelming demand for "Operational Tools over Policy Theory." Economies expressed a strong preference for practical support mechanisms—specifically "situational checklists," "template agreements," and "concise guidance"—rather than purely policy-oriented reports (Survey Q9, Q11). This validates the project’s focus on practical guidelines and suggests that future work should continue to develop resources that MSMEs can directly apply in their day-to-day operations.

3) Proposals for Future APEC Cooperation

Based on these findings, two areas of future cooperation emerge naturally. These suggested agendas build on existing IPEG practices of information exchange, comparative research, and capacity building. They are designed to be voluntary, member-driven, and research-based, without implying institutional restructuring or creating new standing bodies.

Agenda 1: Deepening Regional Understanding of Digital and AI-Related Risks

As digital and AI-related risks continue to evolve, economies may benefit from further sharing of experiences and analytical findings to close the knowledge gap.

(1) Rationale: To proactively address the "Digital Transformation of Risk" (Insight #1), economies need a mechanism to develop common understandings of emerging technological threats through voluntary exchange.

(2) Possible Voluntary Activities:

- Joint Analytical Work: Conduct member-driven studies examining how AI tools and digital collaboration platforms influence trade secret management and exposure.
- Experience Exchange: Utilize existing IPEG meetings to share recent trends, anonymized case examples, or approaches for handling digital evidence, as appropriate.
- Development of Reference Materials: Create concise reference materials summarizing considerations for dealing with cloud-based or AI-related trade secret risks.

Agenda 2: Strengthening MSME Capacity for Practical Protection and Management

Survey responses show strong demand for simple, actionable guidance to support MSMEs in improving their day-to-day management of trade secrets. This agenda focuses on researching and sharing effective management practices.

(1) Rationale: With "proving misappropriation" identified as the top challenge (Insight #2), there is a need to explore how MSMEs can improve their internal management and record-keeping practices. This aligns with the demand for practical tools (Insight #3).

(2) Possible Voluntary Activities:

- Study on Internal Documentation Practices: Conduct a study on basic internal documentation practices—such as maintaining access logs, confidentiality acknowledgements, or version histories—that MSMEs can adopt to support their ability to demonstrate reasonable secrecy measures.
- Comparative Research on Administrative Support Models: Conduct comparative research on administrative support models existing in some member economies, such as voluntary time-stamping or document certification services. The purpose is to identify features that may be informative for interested members, without implying mandatory adoption.
- Continued Updates to Practical Toolkits: Continue to update practical toolkits, including modular checklists or sector-specific guidance, to reflect the evolving digital and commercial environment.

The findings of this project highlight that while legal frameworks form an essential basis for trade secret protection, practical management capabilities are equally critical—especially in digital, cloud-based, and AI-enabled business environments. By continuing to share analytical insights, practical tools, and comparative experiences within the existing IPEG framework, APEC economies can support MSMEs in adapting to these emerging challenges. This will help strengthen innovation ecosystems and contribute to sustainable and inclusive growth across the Asia-Pacific region.

References

Articles

Andrew Yizhou Liu, "Trade Secrets Protection and Employment of Public Firms: Evidence from the Uniform Trade Secrets Act", Research Policy, Vol.54, No.6 (2025)

Jeong Kwan-Young et al., "2022 Trade Secret Protection Guide Study", KIPO & KOIPA (2022)

Loc Xuan Le, "Vietnam: Protecting Trade Secrets", Tilleke & Gibbins (2016).

Kim Yong-Sup, "A Study on the Scope of Act on Prevention of Divulgence and Protection of Industrial Technology and Trade Secret Act", Hongik Law Review, Vol.19, No.4 (2018)

Matthew Rimmer, "Promethean Dreams: Intellectual Property and Climate Change in the Anthropocene", in Leonie Reins and Alexander Zahar (eds.), 'Climate Technology and Law in the Anthropocene', Bristol University Press (2023)Rob Batty, "Trade Secrets' under New Zealand Law", SSRN Electronic Journal (2017)

Carmel Grace Philip, "Can I just Spill the Beans on my Employer's Trade Secrets? (Part 1)", Thomas Philip, Advocates & Solicitors (2024)

Maria Delia Oxley, "Trade secret laws and regulations in Peru", CMS Expert Guide to Trade Secrets (2021)

Jonathan Chu, "Trade secret laws and regulations in Hong Kong", CMS Expert Guide to Trade Secrets (2022)

Sheena Jacob, "Trade secret laws and regulations in Singapore", CMS Expert Guide to Trade Secrets (2022).

Rob Batty, "Trade Secrets' under New Zealand Law", SSRN Electronic Journal (2017)

Agustín Valencia-Dongo, "Espionaje corporativo en el Perú: el caso del ejecutivo topo", Bullard Falla Ezcurra (2021)

Ivy Liang, "How to protect your trade secrets in South-East Asian countries and China", Gowling WLG (2023)

Shota Watanabe et al., "Current Status of ASEAN Data Governance and Its Implications for the Digital Economy Framework Agreement", ERIA Discussion Paper Series, No.539 (2025)

Reports

Latin America IP SME Helpdesk, 'Trade Secrets in Chile: A guide for EU SMEs', European Commission (2021)

South-East Asia IP SME Helpdesk, 'Case Study 01 – Inexperience of Indonesian courts with trade secret cases', European Commission

South-East Asia IP SME Helpdesk, 'Case Study 28 - Trade Secrets protection in Thailand', European Commission

Ministry of Economy, Trade and Industry (METI) of Japan, 'Trade Secret Management Guidelines', METI (2025).

UNCTAD, 'Gap Analysis of Cyberlaws in Pacific Small Island Developing States', United Nations (2025)

World Intellectual Property Organization, "Overview of National and Regional Trade Secret Systems: Russian Federation", WIPO (2024)

Law Library of Congress, 'Protection of Trade Secrets: Brazil, China, India, Russian Federation, South Africa', CreateSpace Independent Publishing Platform (2014)

RTM Group, 'Анализ судебной практики за 2018-2020 годы по спорам, связанным с нарушением NDA (соглашение о неразглашении)', RTM Group (2021)

Websites

Korean Intellectual Property Office (KIPO);
https://kipo.go.kr/ko/kpoBultnDetail.do?menuCd=SCD0200618&ntatcSeq=19719&aprchId=BUT0000029&sysCd=SCD02#1

Attorney General's Chambers, Prime Minister's Office, Brunei Darussalam;
https://www.agc.gov.bn/AGC%20Images/LAWS/ACT_PDF/cap153.pdf

Innovation, Science and Economic Development Canada;
https://ised-isde.canada.ca/site/canadian-intellectual-property-office/en/trade-secret-theft#Section1

Central Authority of Ontario, Canada;
https://www.ontario.ca/laws/statute/00e41

Supreme Court of Canada;
https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1678/index.do

Intellectual Property Court of the Supreme People's Court of China;
https://ipc.court.gov.cn/zh-cn/news/view-3092.html

National Enterprise Credit Information Publicity System, China;
https://credit.cngy.gov.cn/detail.do?contentId=d4288d717a0241e79deaabb224c3c018&channelId=60a1ca1108aa43af9d48c526404268db

World Intellectual Property Organization, WIPO
https://www.wipo.int/en/web/business/w/news/2025/startups-and-smes-in-viet-nam-leveraging-ip

World Intellectual Property Organization, WIPO Lex;
https://wipolex-resources-eu-central-1-358922420655.s3.amazonaws.com/edocs/lexdocs/laws/en/id/id041en_1.pdf
https://www.wipo.int/wipolex/en/legislation/details/15707
https://www.wipo.int/wipolex/en/legislation/details/15720
https://www.wipo.int/wipolex/en/legislation/details/19564
https://www.wipo.int/wipolex/en/legislation/details/20816
https://www.wipo.int/wipolex/en/legislation/details/22547

World Trade Organization;
https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_362.pdf

Andean Ministerial Platform on Intellectual Property;
https://www.ampeid.org/documents/regional/decision-no-486-of-the-andean-community-commission-establishing-the-common-regime-on-industrial-property/#:~:text=Decision%20486%20establishes%20the%20new%20legal%20framework%20for,all%204%20Member%20States%20of%20the%20Andean%20Community.

Central Authority of Peru;
https://cdn.www.gob.pe/uploads/document/file/1664721/DL%201075.pdf.pdf?v=1613011875

Philippine Competition Commission (PCC);
https://www.phcc.gov.ph/file-manager/1/About%20Us/Philippine-Competition-Act-PCA-1.pdf

Taiwan Intellectual Property Office (TIPO);
https://www.tipo.gov.tw/tw/cp-7-976337-4e186-1.html

Bird & Bird Insights;
https://www.twobirds.com/en/insights/2020/australia/an-overview-and-update-on-the-protection-of-trade-secrets-in-australia

Alessandri Abogados, Chile;
https://alessandri.legal/en/trade-secrets-and-current-trends-in-chile/

Simmons & Simmons;
https://www.simmons-simmons.com/en/publications/cm2myu60h0050tqmoirzgodn7/hong-kong-court-client-contacts-not-confidential-in-conpak-v-luk

Drew Network Asia;
https://www.drewnetworkasia.com/newsroom/malaysia-trade-secret-in-employment-perspective/

Pacific Islands Legal Information Institute;
https://www.paclii.org/pg/legis/consol_act/popca1973404/
https://www.paclii.org/cgi-bin/sinodisp/pg/legis/consol_act/cca1974115/index.html?stem=&synonyms=&query=criminal

Viet An Law;
https://vietanlaw.com/learn-about-trade-secrets-in-the-philippines/
https://vietanlaw.com/vietnam-intellectual-property-no-50-2005-qh11/
https://vietanlaw.com/12-2017-qh14-364731/

Lawyer-Philippines.com;
https://www.lawyer-philippines.com/articles/legality-of-non-disclosure-agreements-in-employment-contracts-in-the-philippines

Law.asia;
https://law.asia/trade-secret-laws-philippines-taiwan-legal-trends/

State Administration for Market Regulation (SAMR);
https://www.gov.cn/zhengce/zhengceku/2022-03/23/content_5680784.htm

Minhang District People's Government Office;
https://www.shanghai.gov.cn/gwk/search/content/deb01b7c2d6b494396d5bf6a66e9a7b5

Shijiazhuang Municipal People's Government Office;
https://www.sjz.gov.cn/columns/5e07049d-1b86-4736-af3d-f62945304c23/202507/18/26b69d2e-bb99-4749-88cf-39984056aaf7.html

Yinchuan Municipal People's Government Office;
https://www.yinchuan.gov.cn/zzb/szfwj/202503/t20250303_4843656.html

Korea Trade Secret Protection Center;
https://www.tradesecret.or.kr/main.do

Intellectual Property Office of Singapore (IPOS);
https://www.ipos.gov.sg/about-ip/trade-secret/

Vietnam Intellectual Property Office (IP Vietnam);
https://ipvietnam.gov.vn/web/guest/hot-news-tisc_ip-hub/-/asset_publisher/OVX2E6EdHTmH/content/to-chuc-so-huu-tri-tue-the-gioi-va-cuc-so-huu-tri-tue-trien-khai-chuong-trinh-ao-tao-va-tu-van-quan-tri-so-huu-tri-tue-cho-doanh-nghiep-viet-nam