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

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-03.4

Table of Contents

1. Introduction

Introduction

Small and medium-sized enterprises (SMEs) within APEC member economies play a vital role as key drivers of innovation and industrial growth. While they lead regional economic development through technological innovation and securing market competitiveness, many SMEs still face significant challenges in protecting trade secrets and proprietary technologies. They are particularly vulnerable to technology theft or leakage due to limited human and technical resources.

According to a 2022 survey by the Ministry of Intellectual Property (MOIP), 51.2% of trade secret leaks were caused by former employees, and only 44.8% of all companies implemented preventive measures such as exit interviews or non-disclosure agreements. This result highlights the gap between awareness and practice regarding trade secret protection.

This issue is not unique to Republic of Korea; it is a common phenomenon across APEC member economies. The level of implementation and awareness of trade secret protection systems varies across economies, leading to differences in the level and effectiveness of trade secret protection.

Against this backdrop, this guidebook aims to provide guidance on trade secret management and legal remedies to protect and support the competitiveness of SMEs. Furthermore, by sharing the legal systems and case studies of APEC member economies, it aims to provide foundational reference materials for stakeholders in each economy to improve their own trade secret protection systems.

The core content of the guidebook is structured into four main chapters. Chapter 1 covers the core elements of trade secret management, while Chapter 2 addresses the classification and grading of corporate assets. Chapter 3 addresses contracts with employees, such as non-disclosure agreements, while Chapter 4 describes workplace policies for employees.

Furthermore, the Annex briefly summarizes each economy's legal frameworks, civil remedies, criminal remedies, and cases, enabling stakeholders to compare and understand them more broadly.

However, this guidebook does not aim to present uniform standards or norms. Its purpose is to offer various approaches as reference material that each economy can review and utilize according to its own circumstances. Therefore, the content included in the text should be understood as foundational material that can be flexibly interpreted and supplemented according to internal conditions, and further developed through additional research or institutional review when necessary, rather than as definitive interpretations.

It is hoped that this guidebook will contribute to strengthening the competitiveness and resilience of SMEs in APEC economies and lay the groundwork for sustained mutual learning and cooperation among APEC economies. Furthermore, it is anticipated that this document will serve as a useful starting point and practical reference for each economy to develop a trade secret protection system that aligns with its internal circumstances.

2. Managing Trade Secrets within a Business

I. Key Elements of Trade Secret Management

Introduction

In today's knowledge-driven economy, protecting and managing trade secrets has become a core element of company's competitiveness and long-term sustainability. Unlike patents, which rely on formal registration and public disclosure, trade secrets derive protection from their confidential nature. This makes them highly flexible yet vulnerable to leakage, particularly amid increasing digitalization, globalization, and interconnected business environments.

Trade secrets are legally defined through three fundamental elements: secrecy, economic value, and reasonable confidentiality management. Secrecy requires that the information is not publicly known; economic value reflects its actual or potential commercial significance; and confidentiality management, the most decisive element, requires systematic and proactive measures to maintain secrecy.

Although legal systems and industrial structures vary across the APEC member economies, several foundational practices apply broadly to SMEs. These include clear designation of trade secrets, structured classification, confidentiality obligations for employees and partners, physical and digital access controls, the assignment of responsible personnel, and ongoing security training. Courts in Republic of Korea evaluate whether such measures have been appropriately implemented when determining trade secret eligibility and infringement.

This chapter introduces the related contents. And, as the systems and operational methods vary across economies, this guidebook focuses on elements that can serve as general references. We recommend that detailed implementation methods and system designs be flexibly supplemented and developed to align with each member economies' policy and organizational conditions.

1. Definition and Requirements

1) Definition of Trade Secrets: ① Not publicly known, ② Possessing independent economic value, and ③ Managed as confidential information

2) Scope: Production methods, sales methods, and other technical and managerial information useful for business activities

3) Requirements

- Secrecy: Non-disclosure
- Economic Usefulness: Possessing independent economic value
- Confidentiality: Management in secret

2. Secrecy

1) Meaning: A secret not publicly known

2) State of 'non-disclosure'

- Not known or knowable by the general public
- Not published in public materials like publications and maintained confidentially

3) Information already known within the relevant industry or freely accessible to anyone is not recognized as a trade secret

4) Burden of Proof for Secrecy: Lies with the party alleging infringement (= trade secret holder)

5) Secrecy is not an absolute concept but a relative one

- Not require that the information be completely unknown to anyone
- Secrecy may be recognized even if known within a certain circle of people, provided confidentiality is maintained
- Secrecy may be recognized if a third party only knows the general outline and lacks specific or detailed information

3. Economic Usefulness

1) Meaning

- The holder can use the information to gain a competitive advantage over competitors
- Significant costs and efforts are required to acquire or develop the information

2) Significance

- Not considered a trade secret merely because it is secret
- Must have meaning from an economic perspective

3) Scope of Recognition

- Economic usefulness does not necessarily mean the information itself is the subject of economic transactions
- Information with no possibility of realization is not a trade secret
- As long as the information is kept secret, it is recognized if it has real or potential economic value
- Even if incomplete, it can be a trade secret if usable in business activities

4) Criteria for Determining Economic Usefulness

(1) Provision of Competitive Advantage

- Generates economic benefits such as reduced production costs or enhanced sales efficiency
- Contributes to improved competitiveness relative to competitors

(2) Requirement of Acquisition/Development Costs and Effort

- Requires payment of compensation or usage fees for information use
- Demands significant effort and cost for independent development

4. Confidentiality

1) Meaning: Determines whether the information is being maintained as confidential

2) The most crucial element among the requirements for establishing a trade secret

3) Criteria Adopted by Courts of Republic of Korea

- Whether the company exerted sufficient effort to manage the secrecy (the company's size is also considered)

4) Position of Courts in Republic of Korea

- Does not require excessive secrecy management efforts relative to the company's size
- However, if even a manageable level of effort was absent, the secrecy management effort is deemed insufficient

5) Cases where confidentiality management is recognized

- Indicating or notifying that the information is a trade secret
- Restricting who can access the information or how it can be accessed
- Imposing a duty of confidentiality on those who access the information

4-1. Factors for Determining Confidentiality

1) Designation of Trade Secrets

- Mark trade secrets with labels such as ‘Confidential’

2) Classification of Trade Secret Levels

- Distinguish trade secrets from general information
- Manage trade secrets by classification level

3) Security Training

- Conduct security training for employees

4) Notification of Trade Secrets

- Notify employees of the existence (scope) of trade secrets and confidentiality obligations

5) Obtaining Employee Agreements

- Obtain confidentiality agreements from employees upon hiring and termination

6) Entering Confidentiality Agreements with Business Partners

- Sign confidentiality agreements before conducting business

7) Implementing Security Regulations

- Establish and enforce internal security regulations

8) Designating Security Personnel

- Assign personnel dedicated to trade secrets and company security

9) Restricting access to trade secrets

- Grant access rights to trade secrets on a need-to-know basis
- Record details of trade secret access, use, etc.

10) Installing and operating security devices

- Install and operate CCTV cameras, card readers, etc.

11) Separating development/storage rooms and restricting access

- Operate separate development rooms for producing trade secrets and controlling access
- Operate a separate storage room for trade secrets with access control

12) Security checks upon entry

- Search and inspect personal belongings, IT devices, etc., upon entering the company or controlled areas

13) Restrict copying/transmission of trade secrets

- Restrict copying via removable storage media
- Control file attachments via email

14) Set passwords for computers/networks

- Set computer login and network access passwords

15) Security Software and File Encryption

- Installation and operation of computer security management programs
- Encrypting and storing trade secret files

16) Others

- Installation of shredders and email deletion upon resignation
- Hard disk formatting upon resignation
- Whether regulations exist but are not enforced
- Other factors for assessing confidentiality management

17) Factors considered when determining the confidentiality of court proceedings in Republic of Korea

Category	Enhanced Confidentiality Management	Relaxed Confidentiality Management
Industry	Industries with high frequency of trade secret infringement/leakage incidents	Industries with low frequency of trade secret infringement/leakage incidents
Scale	Cases with a large number of employees Cases with substantial capital Cases with high sales/market share	Fewer employees Less capital Lower sales/market share
Nature of Trade Secret	Rapid development pace in the technology field where the trade secret resides (e.g., semiconductors > agricultural tools) High value of the trade secret Nature of the work where only a small number of personnel need access/viewing rights	When the technological field of the trade secret has a slow pace of development When the trade secret has low value When the nature of the work requires the trade secret to be shared among many employees
Method and Means of Infringement	When trade secret infringement is possible even through simple methods and means	When the method or means of trade secret infringement is sophisticated
Relationship between Infringer and Holder	When trade secret infringement is possible even between the infringer and the holder When the infringer lacks access rights	When there is a high level of trust between the infringer and the holder (e.g., co-founders, long-term employees) When the infringer had access rights
History of Infringement/ Leakage	When there has been a trade secret leakage incident	When there has been no trade secret leakage incident

5. Trade Secret Protection/Management Guidelines (10 Commandments of Trade Secret Protection)

1) Impose trade secret protection obligations on those with access

2) Distinguish between general information and trade secrets

3) Clearly mark information as trade secrets

4) Restrict access/use rights to trade secrets

5) Establish and manage separate locations for developing/storing trade secrets

6) Designate dedicated security management personnel

7) Secure evidence of trade secret management for potential disputes

8) Conduct regular security training

9) Establish and enforce security-related regulations

10) Notify individuals of trade secret status and their duty to protect trade secrets

6. Top 10 Essential Rules for Protecting Trade Secrets in Small and Medium-Sized Enterprises

1) Implement management regulations for trade secret protection

- Classify trade secrets and establish handling procedures
- Define employee obligations
- Establish procedures for storing and disposing of trade secrets
- Operate visitor access control regulations

2) Designate dedicated security management personnel

- Designate a security officer
- Conduct regular trade secret protection audits

3) Conduct regular training on trade secret protection for all employees

- Conduct training every six months or quarterly
- Raising Awareness of the Importance of Trade Secret Protection

4) Have all employees sign confidentiality agreements; have key personnel sign non-compete agreements

- All employees: Sign confidentiality agreements
- Key developers/executives: Additionally sign non-compete agreements

5) Thorough post-employment management for personnel handling trade secrets upon resignation

- Thorough handover of trade secrets upon resignation
- Confirm return of documents/technical information and deletion of files
- Remind of obligations to comply with trade secrets and penalties for violations

6) Classification and separate management of trade secrets

- Identify trade secrets among corporate assets
- Assign and manage classification levels (Top Secret/Secret/Confidential)

7) Strictly manage storage, access, copying, and removal of critical documents

- Store in a separate, locked facility
- Prohibit copying or removal of materials
- Assign and manage control numbers

8) Designate and manage areas housing critical equipment as controlled zones

- Designate development/manufacturing equipment areas as access-controlled zones
- Prohibit bringing in cameras or smartphones
- Install surveillance equipment such as CCTV

9) Deposit of Technical Data

- Protect trade secrets using the technical data deposit system

10) Implement strict security for information systems

- Network authentication and data encryption
- Regular password changes
- Use only authorized USB drives
- Utilize security monitoring services

II. Classifying and Grading Business Assets

Introduction

There are general principles for classifying and grading business assets, especially trade secrets, with an emphasis on practical implementation suitable for companies. Key topics include dispute-related issues, methods for marking confidential information, structured classification models, evaluation procedures, and access control guidelines.

Courts in Republic of Korea assess whether confidentiality requirements have been met by examining how clearly companies distinguish trade secrets from publicly available information. Accurately identifying the specific information at issue and demonstrating its confidential status are essential, as overly broad claims are typically rejected.

Clearly labeling physical and electronic materials with markings such as ‘Confidential’ or ‘Trade Secret,’ and reinforcing them with measures like password protection or encryption, is essential. A systematic classification workflow is also presented, covering asset identification, scoring based on confidentiality criteria, labeling, implementation of protection measures, and periodic review.

Access should be controlled based on defined job roles rather than individual names, ensuring that employees understand their confidentiality responsibilities through training and communication.

This chapter introduces the related contents. As the systems and operational methods vary across economies, this guidebook focuses on elements that can serve as general references. We recommend that detailed implementation methods and system designs be flexibly supplemented and developed to align with each member economies' policy and organizational conditions.

1. Classification by Grade and Key Issues in Disputes

1) In cases of trade secret leakage, courts of Republic of Korea use the fulfillment of confidentiality management requirements as a key criterion for their judgment

- Publicly available information must be distinguished from trade secrets
- After distinction, marking and notification are necessary so that handlers can clearly understand
- Classification itself is not an essential requirement
- Explicit labeling such as “Confidential” or “Trade Secret” is desirable

2) Core Elements of Confidentiality

- Merely the holder's subjective perception of secrecy is insufficient
- Information accessors must also be able to objectively recognize the information as confidential

3) Key Issues in Disputes

- Specification of the infringed information
- Determination of whether the information qualifies as a trade secret
- Courts of Republic of Korea do not acknowledge abstract assertions like “all technical information of our company is a trade secret,” holding that trade secrets must be specifically identified and managed

2. Designation and Marking of Trade Secrets

1) Information Classification and Designation of Confidential Information Requires Regular and Periodic Review

- Because information that was once confidential may later become public knowledge

2) Marking of Record Media

- Marking is required on record media to enable objective recognition of trade secret status
-When managing by classification level, marking should allow identification of management methods via the record media

3) Methods of Confidential Marking

(1) Offline

- Applying ‘Confidential’ stamps, stickers, etc.

(2) Electronic Information

- Entering confidential markings directly into the data
- Setting password restrictions for file access
- Encrypting files, etc.

4) Effect of Marking

- Only specific authors/responsible parties can determine trade secret status
- Employees/outsiders seeing the trade secret marking can halt or abandon external transfer
- Even if leaked, the marking explicitly identifies the material as the company's trade secret

3. Trade Secret Classification Types

1) Basic

(1) Confidential Information

- Information directly linked to corporate survival, restricted to limited personnel such as relevant executives

(2) Restricted Information

- Information restricted to access by only some relevant employees within the company

(3) Internal Use Information

- Information restricted to internal employees only

(4) Public Information (Public)

- Information disclosed both internally and externally

2) Corporate

- Companies may simplify this to 2-3 levels

Classification Level	Detailed Classification Level	Conditions for Classification as Secret
Internal Use Only	**Top Secret (Level 1 Secret)**	- Disclosure would cause substantial loss
		- Disclosure would significantly benefit competitors
		- Must be unique, undisclosed technical information internally and globally
		- Must have an absolute impact on the organization's profits
		- Must be information securing absolute superiority within the industry
	Secret (Level 2 Secret)	- Disclosure would cause considerable loss
		-Disclosure would provide considerable benefit to competitors
		- Secures relative advantage within the industry
		- Critical information concerning mid-to-long-term strategy
		- Information related to new ventures, new products, manufacturing costs, key analytical data
For External Use Only		- Disclosure will result in disadvantage
		- Information that cannot be publicly disclosed
		- Information restricted from disclosure to parties other than those involved

4. Classification Method and Procedure

1) Trade Secret Classification Method

(1) When the volume of trade secret information is vast and the importance of each piece of information varies

- Classifying into multiple levels and establishing/implementing a management system by level is desirable

(2) The higher the secrecy level, the stricter the management required

(3) However, if the volume of trade secrets classified at high levels becomes excessive

- Increased management costs and potential reduction in management effectiveness

(4) Therefore, balanced application and management are necessary during classification

2) Trade Secret Classification Procedure

(1) Identify Subjects

- Technical Information (R&D information, production/manufacturing information, etc.)
- Management Information (HR/General Affairs information, Accounting/Financial information, Purchasing/Sales information)

(2) Grade Calculation

- Sum of scores for each evaluation index
- 5 evaluation indices: Information creation and maintenance costs, Output information level, Information utilization rate, Internal utilization effectiveness, External leakage risk

(3) Classification/Marking

- Special Confidential Information (Confidential)
- Grade 1 Secret Information (Restricted)
- Grade 2 Internal Use Information (Internal Use)
- Grade 3 Public Information (Public)

5. Practical Procedures for Trade Secret Classification (Example)

1) Assess Current Status

- The company's trade secret protection management system and infrastructure
- Top management's commitment and available resources (budget and personnel)
- Employees' awareness level regarding trade secret protection

2) Identify Subjects

- Technical information (R&D information, production/manufacturing information, etc.)
- Management information (HR/general affairs information, accounting/financial information, purchasing/sales information)

3) Task Force Organization

- Designate a trade secret classification manager and responsible personnel
- Discuss trade secret classification criteria and scope
- Establish a schedule for each stage of trade secret classification
- Develop protection and management plans by classification level

4) Relevant Training or Briefing

- Train employees on the necessity of trade secret classification
- Explain trade secret classification criteria and judgment methods

5) Classification Assessment

- Execute classification
- Compile classification results
- Conduct GAP analysis (verify compliance with classification criteria, absence of bias toward specific classifications, etc.)

6) Protection Management

- Apply classification markings
- Implement protection management measures by classification

7) Monitoring and Improvement/Supplementation

- Collect cases where business efficiency is hindered
- Collect and analyze cases requesting classification adjustments
- Audit for violations of relevant regulations and policies
- Identify improvements for the existing classification system

6. Confidentiality Levels for Corporate Information and Management Measures by Level

1) Standard confidentiality classifications for each type of information commonly held by companies, categorized by type (example)

Classification	Category	Information List	Level
Personnel	Recruitment Information	Applicant Application Form, Employment Contract	Level 2 Confidential
	Personnel Management Information	Employee Personal Information, Personnel Record Cards, Payroll Information, Wage Information, Annual Salary Information, Bonus Information, Job Analysis Information, Organizational Chart	Level 2 Confidential
		Employee attendance information, commuting information, leave of absence information, reinstatement information, retirement information	Level 3 Public
	Personnel transfer information	Personnel assignment information	Level 3 Public
	Personnel evaluation information	Personnel Evaluation Reports, Employee Reward and Punishment Management Information, Employee Reward and Disciplinary Information	Level 2 Confidential
	Training and Education Information	Training Plan Information, Training Results Report	Level 3 Public
	Employee Benefits Information	Employee Benefits Information	Level 3 Public
	Industrial Health Information	Fire Management Information, Industrial Accident Insurance Information	Level 3 Public
	Union Information	Union Membership Information, Union Member Information, Union Negotiation Information, Collective Bargaining Information	Level 3 Public

Classification	Category	Information List	Level
General Affairs	Business Plan Information	Mid-to-long-term management plans, investment plan information, new investment plans	Level 1 Top Secret
	Management Diagnosis Information	Management Diagnosis Report	Level 2 Confidential
	Management performance information	Management Performance Report, Management Analysis Report	Level 2 Confidential
	Management Audit Information	Internal Audit Report, External Audit Report	Level 2 Confidential
	Executive Meeting Information	Executive Meeting Minutes	Level 1 Top Secret
	Board of Directors Information	Board of Directors Roster	Level 2 Confidential
		Board Meeting Minutes	Level 1 Top Secret
	Shareholders' Meeting Information	Minutes of Shareholders' Meetings	Level 3 Public
General Affairs	Tangible Asset Information	Building Register, Office Layout Diagram, Equipment Information, Furnishings Information, Consumables Information	Level 3 Public
		Protected Area Information	Level 2 Confidential
	Intangible Asset Information	Company regulations, corporate rules, work procedures, work manuals	Level 2 Confidential
		Purchase Contracts, Sales Contracts, Service Contracts, Product Development Contracts	Level 3 Public
	Business Systems	Personal computers, networks, databases	Level 2 Confidential
	Security System Information	Security System Information	Level 2 Confidential

Classification	Category	Information List	Level
Accounting	Fund Planning Information	Fund Planning, Fund Balance Planning	Level 1 Top Secret
	Funds Execution Information	Fund Status Information, Fund Settlement Information, Deposit/Withdrawal Information	Level 2 Confidential
	Sales and Purchase Information	Account information, ledger information, book information, vouchers, transaction statements, tax invoices, settlement information, audit reports, financial statements, settlement reports, settlement profit and loss data	Level 2 Confidential
	Product cost information	Cost analysis, Margin rate, Component unit price list, Part-by-Part Transaction Price List, Item-by-Item Price Status, Selling Price, Sales Price	Level 1 Top Secret
	Financial Performance Information	Financial Performance Report, Business Profitability Report	Level 1 Top Secret
	Tax Information	Corporate Tax, Value-Added Tax	Level 3 Public
	Local Tax Information	Acquisition Tax, Registration Tax	Level 3 Public
	Tax Adjustment Information	Tax Adjustment Statement	Level 3 Public
Research Development	Research and Development Information	Research and Development Plan, New Product Development Plan	Level 1 Top Secret
		Research and Development Budget Information	Level 2 Confidential
	Research Results Information	Research and Development Reports, Research and Development Outputs, Research and Development Products, Research and Development Services, Experimental Results, Prototype Performance Testing, Pharmaceutical Efficacy Testing	Level 1 Top Secret
		Research and Development Notes, Development Meeting Minutes, Development Product History	Level 2 Confidential
		Research materials, experimental materials	Level 3 Public

Classification	Category	Information List	Level
Research Development	Industrial Property Rights Management Information	Patents, Utility Models, Designs, Product Image Information, Corporate Image Information	Level 2 Confidential
	Research and Development Utilization Information	R&D Output Utilization Plan	Level 2 Confidential
	Technology Transfer Information	Technology Implementation Agreement, Technology Cooperation Agreement, Technology Transfer Agreement	Level 2 Confidential
	Raw Material and Component Purchase Information	Material Specifications, Raw Material Information, Material Order Information, Material Delivery Information, Purchase Forms, Unit Price Files, Inventory Information, Purchasing Company Information, Subcontractor Information, External Company Investigation and Evaluation Materials	Level 3 Public
Purchasing	Raw Material Purchase Information	Purchasing plan information, material requirements planning information, parts requirements list	Level 2 Confidential
	Business Service Information	Service Plan, Service Report	Level 3 Public
Production and Manufacturing	Production Planning Information	New Product Production Plan, Trial Production Plan	Level 2 Confidential
	Production Equipment Inventory Information	Production Equipment Inventory Status, Production Equipment List	Level 3 Public
	Production Facilities Layout Information	Production Equipment Layout Diagram, Machinery Layout Diagram, Workshop Layout Diagram, Production Equipment Layout Drawing, Product Production Line Design Drawing	Level 2 Confidential
	Production Equipment Operation Information	Production Equipment Operation Status	Level 2 Confidential

Classification	Category	Information List	Level
Production Manufacturing	Production Facilities Inspection Information	Production Equipment Inspection Status, Production Equipment Maintenance Status, Production Device Inspection Status, Production Device Maintenance Status	Level 3 Public
	Production Plant Information	Production Plant Design Drawings	Level 2 Confidential
		Production process design drawings, work methods, work standards, work standard list, integrated process files	Level 2 Confidential
	Production Technology Information	Production drawings, product drawings, manufacturing methods, product processing methods, product assembly methods, product formulation methods, product formulation sequence, product formulation ratios, technical specification drawings, source code, circuit diagrams, PCB layouts	Level 1 Top Secret
	Factory progress information	Work instructions	Level 2 Confidential
		Daily work reports	Level 3 Public
	Product Production Performance Information	Product Production Volume, Product Production Quality, Product Inspection Standards, Product Defect Rate, Defect Improvement Meeting Minutes	Level 2 Confidential
Sales	Product Market Information	Product Market Reports, Market Research Data	Level 2 Confidential
	Sales Information	Sales Plans, Sales Strategies	Level 1 Top Secret
	Public Relations Information	Promotional Materials, Corporate Introduction Materials, Product Introduction Materials	Level 3 Public
	Customer Information	List of Business Partners, Customer Roster, Customer Data Directory, Business Partner Contact Information, Delivery Destination Information, Sales Amounts by Business Partner, Product Delivery Unit Price, Product Delivery Date	Level 1 Top Secret
	Bid Information	Potential Business Partners' Purchase Intentions, Business Feasibility Information, Purchase Specifications, Budget Allocation	Level 2 Confidential

Classification	Category	Information List	Level
Sales	Inspection information	Inspection report, inspection results	Level 2 Confidential
	Sales performance information	Sales Performance Report, Order and Delivery Status, Sales Performance Report	Level 1 Top Secret

2) Trade Secret Management Measures by Classification Level (Example)

Category		Top Secret	Level 1 (Confidential Information)	Level 2 (Restricted Information)	Level 3 (Public Information)
Institutional Management	General Information and Trade Secrets	Trade Secrets			General Information
	Marked as a trade secret so anyone can recognize it	"Top Secret" designation	"Confidential" designation	"For External Use Only" Mark	-
	Designated Security Management Personnel Designation	Common			
	Security-Related Regulations Establishment and Enforcement	Common			
Human Resource Management	Accessibility to Impose Duty to Protect Trade Secrets Protection Obligations Imposed	Imposing a duty of care - Imposing a duty of protection			-
	Implementation of regular security training Implementation	Common			
	Notification of trade secret applicability and protection obligations	Periodic	Once a year	Upon Hire· Upon Resignation	-

<table>
<tr><th colspan="2">Category</th><th>Top Secret</th><th>Level 1 (Confidential Information)</th><th>Level 2 (Restricted Information)</th><th>Level 3 (Public Information)</th></tr>
<tr><td rowspan="4">Physical Management</td><td rowspan="2">Separate trade secret Development· Storage Location Designation and Management</td><td colspan="3">Establishment and operation of access control systems and security systems</td><td>-</td></tr>
<tr><td colspan="3">Development· Designation and Management of Storage Locations</td><td>-</td></tr>
<tr><td>Restriction of access and usage rights for trade secrets</td><td>Some Managers</td><td>Some administrators</td><td>Internal employees</td><td>-</td></tr>
<tr><td>Preparing for disputes Trade secret management Evidence preservation</td><td>Regular</td><td>Periodic</td><td>Upon Change</td><td>-</td></tr>
</table>

7. Designation of Access Authorized Personnel by Level

1) One of the core elements of trade secret management is limiting access authorized personnel

2) Set access permissions by level based on job title and require handling according to confidentiality regulations

3) It is efficient to identify access authorized personnel based on job title rather than individual names (proper nouns)

- Eliminates the need for frequent list revisions when employee composition changes

4) Access holders must recognize their duty to handle trade secrets appropriately as confidential information

5) To this end, conduct training and education

- Clearly communicate trade secret handling regulations to all employees
- Ensure each individual clearly understands the importance and responsibility of the trade secrets they have

III. Contracts with Employees, Such as Non-Disclosure Agreements

Introduction

Effective trade secret protection relies heavily on employee-related contractual mechanisms, particularly confidentiality and non-compete agreements. Because employees directly interact with sensitive information, explicit confidentiality obligations are essential, and courts often view signed agreements as key evidence of proper management.

New-hire confidentiality agreements form the foundation of awareness and compliance. They should specify the scope of trade secrets, define prohibited acts, and inform employees of controlled areas and restrictions on copying or transmitting sensitive data. For experienced hires, employers should verify pre-existing confidentiality obligations to avoid accidental violations.

During employment, confidentiality obligations must be reinforced—especially when employees change roles or gain access to new categories of trade secrets. Non-compete agreements serve as a complementary measure, preventing employees with access to high-value secrets from joining competitors or launching competing businesses. Such agreements must be reasonable in duration, scope, and geographic reach.

The departure stage poses substantial risk. Companies should verify the return or deletion of confidential materials, reaffirm continuing obligations, and conduct structured exit procedures. Additional steps such as access-log review or digital evidence preservation further mitigate leakage risks. Together, these contractual measures provide a lifecycle-based framework that enhances organizational protection and legal defensibility.

This chapter introduces the related contents. And, as the systems and operational methods vary across economies, this guidebook focuses on elements that can serve as general references. We recommend that detailed implementation methods and system designs be flexibly supplemented and developed to align with each member economies' policy and organizational conditions.

1. Confidentiality Obligation

1) Employees' Duty of Confidentiality

(1) Company employees share a collective responsibility to maintain the ‘confidentiality’ of trade secrets designated by the company

(2) This means they are subject to the duty of confidentiality

- However, merely asserting it as an ancillary obligation in the employment contract makes it difficult to recognize it as trade secret management

2) Necessity of Imposing Confidentiality Obligations

(1) It is necessary to impose confidentiality obligations on individuals who may handle or access materials containing trade secrets

(2) Court Precedents in Republic of Korea: The court stated that if a company did not obtain a confidentiality agreement or pledge, it would be difficult to recognize it as personnel management

(3) Whether an employee signed a confidentiality pledge is a factor courts often consider when determining what information was kept confidential

2. Confidentiality Agreement for New Hires

1) Necessity

- The confidentiality agreement is the most fundamental form for protecting a company's trade secrets and other business assets
- It serves as a concrete basis for making employees aware of the importance of protecting trade secrets and their duty to maintain confidentiality, while imposing various obligations for trade secret protection
- It is advisable to obtain a confidentiality agreement from all new employees

2) Required Information and Precautions

(1) Include the employee's department, name, date of birth, and hire date

(2) For the confidentiality agreement to be effective, employees must be informed what constitutes trade secrets

- Vaguely stating “all information the company protects as confidential” is not advisable
- The wording may vary depending on the type of trade secrets or business assets each company needs to protect

(3) The types and content of information protected as trade secrets vary by industry, leading to differences in specific wording and protection methods

- It is practically very difficult to list all the company's trade secrets in a non-disclosure agreement
- Beyond the information examples provided in the standard form, the following content can be referenced and added to the non-disclosure agreement based on the industry

Industry	Content
Electrical· Electronics	Development plans, personnel involved, testing methods, source code, and related information for software that the company plans to develop, has developed, or is currently developing
Chemical	Development and clinical trial plans, development personnel, clinical trial participants and methods, raw materials· formulation ratios· production processes, licensing matters, and related information for pharmaceuticals or medical supplies that the company plans to develop, has developed, or is currently developing
Wholesale/Retail/Service	Cost and pricing information for products the company sells or plans to sell, sales and promotional strategies, contact persons at suppliers or customers· contact information· contact methods, licensing information, and other business information related to business partners
Food and beverage manufacturing	The types and sources of raw materials used in the company's products, raw material ratios, production processes and factory layouts, manufacturing manuals, design drawings, molds, and the product development process

(4) Imposing a duty of confidentiality on new hires regarding information protected as trade secrets or business assets

- Obligate them not to disclose or reveal such information to others

(5) It is necessary to clearly establish that trade secrets and similar information are assets owned by the company

- Because it is common for employees to mistakenly believe that trade secrets acquired during their employment belong to them personally

Aren't trade secrets naturally owned by the company?
- Trade secrets encompass not only technical information but also management information. Therefore, if the content of a trade secret constitutes an 'invention,' it can be treated as a 'work-related invention'; if it constitutes a 'copyrighted work,' it can be treated as a 'work-made-for-hire'. - Under the Patent Act, inventions are generally attributed to the inventor. This is known as the 'inventor principle'. However, for 'service inventions', if a contract or work regulations are established in advance, transferring the right to obtain patents, etc., after consultation with employees, the rights can be attributed to the employer, i.e., the company (Invention Promotion Act Article 10). - Conversely, the Copyright Act stipulates that the author of a 'work made for hire' is the corporation or entity, unless otherwise specified by contract or work rules (Copyright Act Article 9). - For trade secrets constituting technical information, ownership may vest in the company if the company acquires them through contracts or work regulations, similar to 'work-related inventions'. - For trade secrets constituting management information, the outcome may vary depending on the type. If it is a 'copyrighted work' published in the name of the corporation, the company may become the rights holder as stipulated by the Copyright Act. However, even if a computer program is not 'published in the name of the corporation or other entity', the corporation becomes the copyright holder.

(6) It is necessary to explain where the company's controlled areas or facilities are located and what information is permitted for new hires

(7) It must be clearly communicated that actions such as copying trade secret materials obtained in the course of work violate trade secret management regulations

(8) Caution is required as recent cases show increasing instances where companies suffer damage not only from leaks of their own trade secrets, but also from experienced hires or employees illegally obtaining and disclosing others' trade secrets

- Verify what confidentiality obligations experienced hires bear from their previous employers
- It is advisable to preemptively block risks arising from trade secret infringement

[Table 1] Sample Non-Disclosure Agreement for New Hires

Security Pledge Agreement

While employed by (or during my vacations) _____ Co., Ltd (hereinafter "company"), I pledge as follows to protect the company's trade secrets.

1. I confirm that the company has ownership of the technologies and information acquired in connection with my work, either independently or jointly or by third parties, created, produced, developed, designed or devised, including equivalent products.

2. I confirm that the following information corresponds to the trade secrets or business assets of the company, and that I am fully responsible for thoroughly complying with the principles and policies related to the company's employment rules and trade secret management regulations.

① Information written on trade secret management regulations and other internal regulations of the company

② Information marked as trade secrets

③ Records, media, documents, items and information stored in restricted areas, computer systems with limited access, storages with locks

④ Technological and managerial information managed by the company as trade secrets using means other than the aforementioned ①, ②, ③

3. Except for the purpose of performing works assigned to me by the company, I will not use the company's trade secrets and major business assets for personal purposes regardless of reason. I will not disclose trade secrets and business assets to third parties in and out of the company. (Notwithstanding the above, exceptions can be made if prior written consent is granted by the company or if a regulation on the protection of trade secrets allows such use or disclosure.)

4. I will never approach unauthorized information or facilities. I will always follow the company's security regulations, guidelines and policies.

5. I will not copy, record, shoot, cloud upload, send personal email, upload personal SNS or any other form of reproduction or leakage by other means, except for use in the designated work for the company's trade secrets. I will not have any copies of this personally. (Notwithstanding the above, exceptions can be made if prior written consent is granted by the company or if a regulation on the protection of trade secrets allows such duplication or possession.)

6. I will use information processing devices and information communication networks such as the company's computers for business purposes. I understand and agree that
(1) the company may monitor information such as the details of using information processing devices (such as computers) or information communication networks (such as the internet) in case it is necessary to prevent the leak of technology and information that might damage the company.
(2) the company may peruse the details of such information in case of risks of illegal action or infringement of trade secrets.

7. I will not work for the following companies, research institutes, or have any other cooperative relationships (partners, coworkers, advisors, etc.) for [ ] years during and after retirement.
(1) Companies or research institutes that currently sell or are likely to sell the same or similar products. Companies that currently selling and those that are to be sold (whether or not there is a possibility of using the company's trade secrets)
(2) Companies or research institutes that have a substitute effect or market segmentation effect on the company's business (whether or not there is a possibility of using the company's trade secrets)
(3) If this does not apply to Paragraph (1), (2), Companies or laboratories that are significantly more likely to use the company's trade secrets

8. If I violate Article 7, I pledge to reimburse the company immediately for [ ]. If the actual damages exceed the above amount, I will compensate for any excess damages.

9. Even after I leave the company, I will neither reveal nor disclose the trade secrets or business assets I have acquired over the course of my work to a third party using any means, unless the company grants its prior consent.

10. While I work for or even after I leave the company, I will actively cooperate with the company if legal disputes occur in regard to the authority of works assigned to me.

11. I will not provide or disclose company information that are business secrets of others acquired before or during my work for the company. If I find it inevitable to disclose such information to the company, I will consult with the company in advance so the business secrets of others will not be infringed.

12. When I leave the company, I will return all information related to the company's business secrets, as well as all materials related to the major business assets of the company (including tangible and intangible information) that may influence the company's R&D, marketing and property. I will not personally hold any kind of copy in any form related to the information and materials above, and pledge to destroy anything that cannot be returned.

13. In the event of any dispute related to this Agreement, I will try to resolve it smoothly in mutual consultation with the company. If not, I will resolve it through the mediation procedure of the Industrial Technology Dispute Resolution (Settlement) Committee.

I hereby pledge to faithfully comply with the above. If the company suffers harm due to my violation of the pledges above, I will submit to measures per the Unfair Competition Prevention and Trade Secret Protection Act, as well as other related laws and the company's regulations. I will also compensate the company for financial losses incurred, and assume full civil and criminal responsibility.

Date:

I hereby confirm and understand the above, and sign this pledge

Department: _____

Name: _____(Signature)

Date of birth: _____

_____Co., Ltd.

3. Confidentiality and Non-Compete Agreement for Current Employees

1) Non-Disclosure Agreement

(1) Necessity

- Non-Disclosure Agreement for current employees
- Even if signed upon hiring, it is advisable to periodically obtain a Non-Disclosure Agreement during employment
- Reason for regularly obtaining confidentiality agreements from current employees: To heighten awareness of trade secret protection by reminding them that various information acquired during work constitutes the company's trade secrets
- Particularly, as the specific trade secrets an employee becomes aware of may change due to promotions or job reassignments, the confidentiality agreement must be obtained with those specific details

(2) Required Information and Precautions

- Trade secrets should be described more specifically upon hiring
- This is because, upon hiring, duties may not yet be clearly defined, so trade secrets are typically described quite broadly
- It is advisable to list the names and brief descriptions of the company's trade secrets related to the employee's duties and those acquired during their performance
- Even if a company has obtained a security memorandum or confidentiality agreement from an employee, there have been cases where the court ruled that the agreement “merely imposed a general and abstract duty of confidentiality” and thus did not protect the information as a trade secret. Therefore, particular caution is required

[Table 2] Sample Employee Confidentiality Agreement

Security Pledge Agreement

Department:

Name:

As a staff member/employee of [ ] Co., Ltd. (hereinafter "company"),
I pledge as follows to protect the company's trade secrets and marketing assets.

1. I confirm that the company has ownership of the technologies and information acquired in connection with my work, either independently or jointly or by third parties, created, produced, developed, designed or devised, including equivalent products.

2. I clearly understand that any and all information or data acquired over the course of doing my work (write specific work), as written below, constitute the company's trade secrets or major marketing assets.

NO	Trade secrets (or major marketing assets)	Notes
1		
2		
3		
4		
5		

3. In addition to the information in Article 2, the following information shall be confirmed to be the company’s trade secrets or operating assets, and shall be fully complied with and responsible for the relevant policies or policies, such as the employment rules and the regulations for the management of trade secrets.

① Trade Secret Management Regulations, other technical and management information that the Company manages as a trade secret in accordance with the company's internal regulations.

② Information showing trade secrets, confidential information, etc.

③ Restricted zones, computers with limited access, recording media stored in locked lockers, documents, objects, information, etc.

4. Except for the purpose of performing works assigned to me by the company, I will not use the company’s trade secrets and major business assets for personal purposes regardless of reason. I will not disclose trade secrets and business assets to third parties in and out of the company. (Notwithstanding the above, exceptions can be made if prior written consent is granted by the company or if a regulation on the protection of trade secrets allows such use or disclosure.)

5. I will never approach unauthorized information or facilities. I will always follow the company’s security regulations, guidelines and policies.

6. I will not copy, record, shoot, cloud upload, send personal email, upload personal SNS or any other form of reproduction or leakage by other means, except for use in the designated work for the company’s trade secrets. I will not have any copies of this personally. (Notwithstanding the above, exceptions can be made if prior written consent is granted by the company or if a regulation on the protection of trade secrets allows such duplication or possession.)

7. I will use information processing devices and information communication networks such as the company’s computers for business purposes. I understand and agree that:

(1) The company may monitor information such as the details of using information processing devices (such as computers) or information communication networks (such as the internet) in case it is necessary to prevent the leak of technology and information that might damage the company.
(2) The company may peruse the details of such information in case of risks of illegal action or infringement of trade secrets.

8. I will not work for the following companies, research institutes, or have any other cooperative relationships (partners, coworkers, advisors, etc.) for [ ] years during and after retirement.

(1) Companies or research institutes that currently sell or are likely to sell the same or similar products. Companies that are currently selling and those that are to be sold (whether or not there is a possibility of using the company’s trade secrets).

(2) Companies or research institutes that have a substitute effect or market segmentation effect on the company's business (whether or not there is a possibility of using the company's trade secrets)
(3) If this does not apply to Paragraph (1), (2), Companies or laboratories that are significantly more likely to use the company's trade secrets

9. If I violate Article 8, I pledge to reimburse the company immediately for [ ]. If the actual damages exceed the above amount, I will compensate for any excess damages.

10. Even after I leave the company, I will neither reveal nor disclose the trade secrets or business assets I have acquired over the course of my work to a third party using any means, unless the company grants its prior consent.

11. While I work for or even after I leave the company, I will actively cooperate with the company if legal disputes occur in regard to the authority of works assigned to me.

12. I will not provide or disclose company information that are business secrets of others acquired before or during my work for the company. If I find it inevitable to disclose such information to the company, I will consult with the company in advance so the business secrets of others will not be infringed.

13. When I leave the company, I will return all information related to the company's business secrets, as well as all materials related to the major business assets of the company (including tangible and intangible information) that may influence the company's R&D, marketing and property. I will not personally hold any kind of copy in any form related to the information and materials above, and pledge to destroy anything that cannot be returned.

14. In the event of any dispute related to this Agreement, I will try to resolve it smoothly in mutual consultation with the company. If not, I will resolve it through the mediation procedure of the Industrial Technology Dispute Resolution (Settlement) Committee.

I hereby pledge to faithfully comply with the above. If the company suffers harm due to my violation of the pledges above, I will submit to measures per the Unfair Competition Prevention and Trade Secret Protection Act, as well as other related laws and the company's regulations. I will also compensate the company for financial losses incurred, and assume full civil and criminal responsibility.

Date:

I hereby confirm and understand the above, and sign this pledge.

Signed by: _____(Signature)

_____Co., Ltd.

2) Non-Compete Agreement

(1) Meaning

- An agreement stipulating that the employee shall not engage in competitive acts, such as employment with a company competing with the employer or establishing and operating a competing business
- Also referred to as a ‘non-compete agreement’
- The duty of confidentiality and the non-compete obligation are distinct
- The duty of confidentiality and non-compete obligations for former employees should, in principle, be governed by separate agreements

(2) Necessity

- Often entered into because there is a risk that an employee leaving the company may disclose trade secrets acquired during employment if they join a competitor
- To prevent employees from transferring to a competitor or using the company's trade secrets to start their own business by informing them of the obligations in advance while they are still employed

(3) Method of Execution

- It is advisable to execute in written form
- It is advisable to execute the confidentiality and non-compete obligations using a separate form
- It is preferable to execute as a separate agreement rather than including it in an employment contract or collective bargaining agreement

(4) Parties Subject to Execution

- It is acceptable not to execute if there is no possibility of trade secrets being disclosed even if the employee moves to a competitor

(5) Content of Execution

- Period/compensation for the non-compete, geographic scope, prohibited occupations
- Should vary based on how much trade secret information a specific employee possesses and the value of the trade secrets the employee knows

- Agreements imposing excessive burdens on employees, such as setting indefinite or excessively long periods, are highly likely to be deemed invalid by courts in Republic of Korea
- The terms should be mutually agreed upon to achieve a reasonable balance between the employer's interests and the employee's interests

(6) Non-Compete Period

- Determined by considering the employer's interests to be protected (e.g., the value of the secret, the employee's position prior to resignation, the circumstances leading to resignation, whether compensation was paid to the employee, etc.)
- Courts of Republic of Korea may shorten the period or deem the agreement itself invalid if they determine it is excessively long, weighing various circumstances on a case-by-case basis, even if agreed upon by the parties

(7) Compensation for Non-Competition

- Companies are not necessarily required to provide separate compensation for non-competition obligations
- Failure to provide separate compensation does not automatically render the non-compete agreement invalid
- However, courts of Republic of Korea consider whether compensation was paid as a factor in determining the validity of a non-compete agreement
- If a company paid compensation to the employee for the non-compete obligation, the agreement is more likely to be deemed valid compared to cases where no compensation was paid

(8) Validity of Non-Compete Agreements

- Non-compete agreements inherently restrict employees' constitutional freedoms
- Therefore, courts of Republic of Korea assess their validity from a highly stringent perspective
- Courts of Republic of Korea consider whether the employer has sufficiently compelling interests to justify imposing a non-compete obligation on the employee, weighing all relevant circumstances

[Table 3] Non-Compete Agreement Sample

Sample Non-Compete and Non-Solicitation Agreement

This is an Agreement between [NAME OF EMPLOYEE] ("You") and [NAME OF COMPANY] ("Company"). The Agreement is effective on ____ ("Effective Date").

In consideration of the employment opportunity provided by [NAME OF COMPANY], You, intending to be legally bound, agree to the following:

1. **Term of Agreement.** This Agreement is effective on the Effective Date, and shall remain in effect throughout the term of your employment with the Company and for a period of one year thereafter.[1]
2. **Limitations of this Agreement.** This Agreement is *not* a contract of employment. Neither You nor the Company are obligated to any specific term of employment. This Agreement is limited to the subject matter of covenants not to compete or solicit as described in this Agreement.
3. **Covenant Not to Compete.** You agree that at no time during the term of your employment with the Company will you engage in any business activity which is competitive with the Company nor work for any company which competes with the Company.

   For a period of one (1) year immediately following the termination of your employment, You will not, for yourself or on behalf of any other person or business enterprise, engage in any business activity which competes with the Company within _____ miles of the facility in which you were employed.[2][3]

4. Non-solicitation. During the term of your employment, and for a period of one (1) year immediately thereafter, You agree not to solicit any employee or independent contractor of the Company on behalf of any other business enterprise, nor shall you induce any employee or independent contractor associated with the Company to terminate or breach an employment, contractual or other relationship with the Company.

---

[1] Covenants not to compete are not favored by courts, so they generally are interpreted very narrowly. They must be "reasonable" in terms of duration and the geographical area to which they apply. Sometimes the duration can be as long as two or three years, while the size of the territory can be quite small, e.g., a 25-mile radius, or quite large, e.g., anywhere in the world.

[2] Many companies market across the economy and even worldwide, so a narrow restriction may not be terribly helpful. If you seek to limit activity anywhere within a specific economy or anywhere in the world, you will probably need to make the restriction much narrower. You cannot, of course, deprive the employee of a way to earn a living in your industry.

[3] An alternative clause is:

> During the course of your employment, You agree not to work for or provide any services to any competitor of the Company. Neither shall You engage in any competitive activity with respect to the Company. Competitive activity includes, but is not limited to, forming or making plans to form a business entity to directly compete with any business of the Company. This provision does not prevent You from seeking or obtaining employment or other forms of business relationships with a competitor after termination of employment with the Company so long as such competitor was in existence prior to the termination of your relationship with the Company and You were in no way involved with the organization or formation of such competitor.

5. Soliciting Customers After Termination of Agreement.

For a period of one (1) year following the termination of your employment and your relationship with the Company, You shall not, directly or indirectly, disclose to any person, firm, or corporation the names or addresses of any of the customers or clients of the Company or any other information pertaining to them. Neither shall you call on, solicit, take away, or attempt to call on, solicit, or take away any customer of the Company on whom You have called or with whom You became acquainted during the term of your employment, as the direct or indirect result of your employment with the Company.

6. Injunctive Relief.

You hereby acknowledge (1) that the Company will suffer irreparable harm if You breach your obligations under this Agreement; and (2) that monetary damages will be inadequate to compensate the Company for such a breach. Therefore, if You breach any of such provisions, then the Company shall be entitled to injunctive relief, in addition to any other remedies at law or equity, to enforce such provisions.

7. Severable Provisions.

The provisions of this Agreement are severable, and if any one or more provisions may be determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions and any partially unenforceable provisions to the extent enforceable shall nevertheless be binding and enforceable.

8. Modifications.

This Agreement may be modified only by a writing executed by both You and the Company.

9. Prior Understandings.

This Agreement contains the entire agreement between the parties with respect to the subject matter of this Agreement. The Agreement supersedes all prior understandings, agreements, or representations.

10. Waiver.

Any waiver of a default under this Agreement must be made in writing and shall not be a waiver of any other default concerning the same or any other provision of this Agreement. No delay or omission in the exercise of any right or remedy shall impair such right or remedy or be construed as a waiver. A consent to or approval of any act shall not be deemed to waive or render unnecessary consent to or approval of any other or subsequent act.

11. Jurisdiction and Venue.

This Agreement is to be construed pursuant to the laws of the State of _____. You agree to submit to the jurisdiction and venue of any court of competent jurisdiction in _____ County, [STATE] without regard to conflict of law's provisions, for any claim arising out of this Agreement.

Date_____ **[NAME OF COMPANY]**

By _____

By your signature below you acknowledge that you have read and understand the foregoing Agreement, that you agree to comply with all of the terms of the Agreement, and that you have received a copy of the Agreement.

Date_____ _____

Employee

- Factors for Determining the Validity of Non-Compete Agreements and the Likelihood of Validity by Factor

Judgment Factors		Likelihood of Determining the Validity of Non-Compete Agreements	
		Low	**High**
(1) Employer's Interest		When not a business-critical asset	When it is a trade secret or a business-critical asset
(2) Scope of Non-Competition	**Duration (Approx. 2 years)**	For longer periods	For short-term cases
	Region	When there are no restrictions	When restrictions apply
	Occupation	When there are no restrictions, such as 'all similar industries'	When restrictions apply, such as 'specific business operations'
(3) Payment of compensation		When no compensation is paid	Severance pay, retirement living allowance, security allowance, promotion opportunities, etc.· When intangible compensation is provided
(4) Worker's circumstances	**Position held prior to retirement**	If engaged in work unrelated to trade secrets or other employer interests	If engaged in work related to trade secrets or other employer interests, or if a business partner
	Circumstances of resignation	In cases of simple job change	In cases involving improper purposes such as the disclosure of trade secrets
	Livelihood	When changing jobs is impossible or difficult without utilizing existing knowledge and experience	When changing to another occupation is easy
(5) Necessity for the public interest		Transactions between private parties, narrow markets, small-scale transactions	Indiscriminate recruitment of personnel, disruption of market transaction order, infringement of third-party rights, weakening of the economy's competitiveness, loss of the economy's wealth

4. Confidentiality Agreement for Departing Employees

1) Necessity

- A significant number of trade secret infringement cases are caused by departing employees
- Verify the return of trade secret-related materials through interviews before leaving
- Depending on the importance of the role/position, prepare a separate confidentiality agreement and request a non-compete agreement

2) Required Information and Precautions

(1) Specify the specific employee's hire date, the department, position, and rank held immediately prior to departure, and briefly describe their job duties.

- e.g., (Department/Position/Rank) R&D Team/Team Leader/Grade 2 (Job Description) Development of user interfaces for device information such as mobiles

(2) Instead of vaguely stating “all information acquired during employment,” specifically list the names and brief descriptions of the information constituting trade secrets

(3) Because the non-compete obligation may infringe upon constitutionally guaranteed rights, including an employee’s freedom to choose their occupation under the Korean Constitution, it is permitted only to the extent that reasonable necessity is acknowledged

- The duration, geographic scope, and job type of the non-compete period should be set within reasonable limits based on the employer's interests, whether compensation is provided, and the employee's job duties
- Caution is required as stipulating an excessively long non-compete period, or defining the geographic scope as ‘worldwide’ or the job type as ‘manufacturing industry’ too broadly, may invalidate the non-compete agreement

(4) A predetermined amount of damages shall be stipulated for violations of the confidentiality and non-compete obligations

- This alleviates the burden of proving the amount of damages and ultimately ensures the compliance and effectiveness of the departing employee's confidentiality and non-compete obligations

(5) The obligation to return or destroy relevant materials must be emphasized, and the employee must be made aware that they cannot leak or personally retain such materials

- This is because cases of departing employees unlawfully removing trade secret materials are frequent

(6) Preparations in case trade secret infringement is discovered after an employee's departure

- Even belatedly, email transmission records or computer hard disks should be investigated. However, obtaining consent under the Personal Information Protection Act, etc., will be difficult, so provisions can be made to obtain consent for this upon departure

3) Measures beyond signing non-disclosure agreements

(1) Requires substantive management measures beyond merely signing agreements

- Assign dedicated staff → Return/delete stored files and materials
- Format the hard disk of the computer used by the departing employee
- For data on removable storage devices taken out, require deletion/disposal followed by submission of verifiable data

(2) If possible, it is advisable to verify the following for a certain period before resignation

- Computer usage history
- Access history to controlled areas
- Network access history
- File copy/transfer history, etc.

[Table 4] Sample Non-Disclosure Agreement for Departing Employees

Security Pledge Agreement

(for Departing Employees)

As I leave _____ Co., Ltd. (hereinafter "company") in (specific date), I pledge as follows on the protection of the company's trade secrets and business assets.

1. As a (specific position) of the company conducting (specific works), I have handled the following trade secrets and business assets.

No	Trade secret (or major business asset)	Details
1		
2		
3		

2. In addition to the information in Article 1, the following information shall be confirmed to be the company's trade secrets or operating assets, and shall be fully complied with and responsible for the relevant policies or policies, such as the employment rules and the regulations for the management of trade secrets.

① Trade Secret Management Regulations, other technical and management information that the Company manages as a trade secret in accordance with the company's internal regulations.

② Information showing trade secrets, confidential information, etc.

③ Restricted zones, computers with limited access, recording media stored in locked lockers, documents, objects, information, etc.

3. Except for the purpose of performing works assigned to me by the company, I have not used the company's trade secrets and major business assets for personal purposes regardless of reason. I have not disclosed trade secrets and business assets to third parties in and out of the company.

4. I have never approached unauthorized information or facilities. I have always followed the company's security regulations, guidelines and policies.

5. I have not copied, recorded, shot, cloud uploaded, sent personal email, uploaded personal SNS or any other form of reproduction or leakage by other means, except for use in the designated work for the company's trade secrets. I have not had any copies of this personally. (Notwithstanding the above, exceptions can be made if prior written consent is granted by the company or if a regulation on the protection of trade secrets allows such duplication or possession.)

6. I have used information processing devices and information communication networks such as the company's computers for business purposes. If the company is concerned about tort or trade secret, I understand and agree that the company will be able to access the relevant information.

7. I will not work for the following companies, research institutes, or have any other cooperative relationships (partners, coworkers, advisors, etc.) for [ ] years during and after retirement.

(1) Companies or research institutes that currently sell or are likely to sell the same or similar products. Companies that are currently selling and those that are to be sold (whether or not there is a possibility of using the company's trade secrets)

(2) Companies or research institutes that have a substitute effect or market segmentation effect on the company's business (whether or not there is a possibility of using the company's trade secrets)

(3) If this does not apply to Paragraph (1), (2), Companies or laboratories that are significantly more likely to use the company's trade secrets

8. If I violate Article 7, I pledge to reimburse the company immediately for [ ]. If the actual damages exceed the above amount, I will compensate for any excess damages.

9. Even after I leave the company, I will neither reveal nor disclose the trade secrets or business assets I have acquired over the course of my work to a third party using any means, unless the company grants its prior consent.

10. While I work for or even after I leave the company, I will actively cooperate with the company if legal disputes occur in regard to the authority of works assigned to me.

11. When I leave the company, I will return all information related to the company's business secrets, as well as all materials related to the major business assets of the company (including tangible and intangible information) that may influence the company's R&D, marketing and property. I will not personally hold any kind of copy in any form related to the information and materials above, and pledge to destroy anything that cannot be returned.

12. In the event of any dispute related to this Agreement, I will try to resolve it smoothly in mutual consultation with the company. If not, I will resolve it through the mediation procedure of the Industrial Technology Dispute Resolution (Settlement) Committee.

I hereby pledge to faithfully comply with the above. If the company suffers harm due to my violation of the pledges above, I will submit to measures per the Unfair Competition Prevention and Trade Secret Protection Act, as well as other related laws and the company's regulations. I will also compensate the company for financial losses incurred, and assume full civil and criminal responsibility.

Date:

I hereby confirm and understand the above, and sign this pledge.

Department: _____

Name: _____ (Signature)

_____ Co. Ltd.

IV. Workplace Policies for Employees

Introduction

Robust trade secret protection requires a comprehensive internal management system that governs how sensitive information is created, stored, used, and safeguarded. As digital work environments and external collaborations expand, companies must establish clear regulations, define roles and responsibilities, and maintain consistent security practices.

Core elements of such systems include internal regulations, governance structures, and designated personnel responsible for oversight. Physical materials must be securely stored, transported, copied, and disposed of, while electronic data requires encryption, access restrictions, logging, and a secure network environment. Personal storage devices and unregulated external cloud services should be restricted.

Human resource management plays a critical role, particularly during employee transitions. Dedicated security officers, structured exit interviews, verification of material returns, and evidence preservation are essential for minimizing leakage risks.

Training and awareness programs further strengthen compliance by ensuring employees understand policies and consequences. As remote work becomes more common, companies must adapt regulations, verify remote environments, and implement self-checklists to address new vulnerabilities.

Finally, companies should maintain evidence of their protective measures, such as NDAs, training records, access logs, and trade secret registers, to support legal claims when disputes arise.

This chapter introduces the related contents. And, as the systems and operational methods vary across economies, this guidebook focuses on elements that can serve as general references. We recommend that detailed implementation methods and system designs be flexibly supplemented and developed to align with each member economy’s policy and organizational conditions.

1. Establishment and Operation of a Trade Secret Management System

1) Necessity of Establishing a Management Framework

- To safely and efficiently protect trade secrets, establishing a systematic and organized management framework and system is the top priority
- Necessity to establish trade secret management regulations capable of protecting personnel, departments, information materials, materials, facilities, communications, locations, etc., related to trade secret information required for business activities from competitors and unauthorized parties

2) Establishment of a Dedicated Department

- After establishing regulations, establish a dedicated department for trade secret management tasks
- Functions: Handle all routine tasks including trade secret classification, storage, management, handler authorization/revocation, and management body composition/operation

3) Composition of Trade Secret Management Body

- Role: Research and develop management systems; establish basic guidelines; set key regulations, amendments, approvals, target tasks, and classification criteria; determine protection methods and classification standards; deliberate and confirm fundamental matters like decentralized vs. centralized management approaches

4) Audit and Potential Exemption

- The company must audit employee management practices and take sufficient measures to prevent violations
- If “sufficiently concrete measures to effectively prevent violations” are taken for issues uncovered through audit, the corporation may be exempt from liability for employee violations

5) Inspection and Audit Items

- The inspection and audit items listed below are not necessary and sufficient conditions for exemption
- Failure to meet some items does not automatically result in punishment

Establishment of Management Policies (Basic Policies, Standards, Regulations, etc.)	Management policies (basic policies, standards, regulations, etc.) to prevent misconduct in trade secret management must be established, and procedures to implement them must be in place. However, these need not be separate, independent documents or procedures distinct from other internal control activities. Furthermore, they must be continuously reviewed based on audit results.
Responsible Persons and Clarification the Responsible Party's Authority	There shall be a responsible person who supervises whether the above management policy is properly adhered to, and the existence of this responsible person must be known within the organization. If, for any reason, supervision within a subsidiary· or related company fails to adequately fulfill its role, the responsible person at the parent company shall not neglect this situation. Instead, they shall consult with the relevant subsidiary· or related company to establish necessary countermeasures and, if required, provide reasonable support as the parent company.
Trade Secrets Preventing and Management Policy Thoroughly Communicated	Employees must be thoroughly informed of the aforementioned management policies and procedures by mandating participation in training or seminars on trade secret management, or by distributing documents explaining how to act. However, training· and seminars should be tailored to potential risks specific to each workplace or job role, rather than being uniform for all employees. Furthermore, from the perspective of protecting employees as well as safeguarding trade secrets, it is advisable for the business operator to provide training and education· on self-defense measures, including preventive evidence, to ensure employees are not unjustly suspected of trade secret leaks.
Routinely Monitoring is Conducted.	It is advisable to establish an internal system (e.g., setting up consultation channels) where employees can seek prior advice on whether actions violate laws and regulations. Since routine information gathering activities may sometimes be mistakenly perceived as improper acquisition of trade secrets, it is beneficial to establish an internal channel for consulting whether such actions violate laws and regulations. Furthermore, accumulated consultation cases can be used to review management policies or for employee training and awareness activities. Additionally, during routine business activities, if managers at any level detect unusual technical development or customer growth, or any other clues suggesting the improper acquisition of trade secrets, it is advisable for the organization to verify the source of the information.

Internal Audit Conducted	Conduct risk-based internal audits tailored to the risk of trade secret infringement. Risk-based auditing generally means conducting comprehensive and frequent audits at workplaces where the nature of the work makes violations of the Trade Secrets Protection Act likely to occur, and conversely, conducting limited and infrequent audits at workplaces where this is not the case. However, this must be conducted as an independent activity separate from internal control activities. Furthermore, since internal audits alone cannot be relied upon to detect all problematic conduct, when potential issues are identified through reports from insiders or other means, it is advisable to leverage that experience to re-examine audit items and targets, continuously improving the precision of the audit process.
Post-Incident Response System Establishment	It is important to establish consistent disciplinary standards for trade secret management in advance and ensure employees are fully aware of them. These standards must include measures against those who ordered misconduct, those who participated in misconduct under a superior's orders yet reported their own wrongdoing, and further, the treatment of those who knew about misconduct but failed to report it.

2. Establishment and Implementation of Internal Trade Secret Management Regulations

1) Significance of the Regulations

- Trade secret management regulations are internal rules that explicitly state the company's intent regarding trade secret management
- Court precedents in Republic of Korea also assess a company’s “confidentiality management” based on whether internal regulations have been established and effectively implemented

2) The regulations must include the following

- Identification of trade secrets
- Authorization of responsibilities
- Designation of management personnel
- Management procedures
- Incident response procedures
- Disciplinary procedures and consequences for responsible parties in case of incidents

3) Implementation Measures

- After enactment, post the regulations on the intranet or similar platform to ensure employees can access them at any time
- Conduct ongoing training to ensure employees understand and apply the regulations
- Crucial to implement guidelines: designate trade secret management personnel, conduct training, collect pledges, etc., as per regulations; periodically report management status and make improvements

4) Utilizing the regulations

- The established security regulations can serve as key material for regular security training for employees

5) Precautions

- If regulations are only formally established but not implemented → Courts of Republic of Korea will deem this as a lack of effort in managing secrets
- Substantial implementation is more important than the mere existence of regulations

6) Recommendations for Implementation

- Utilize the “Trade Secret Management Regulations” standard template uploaded on the Trade Secret Protection Center website
- Recommended to modify and supplement according to each company's situation before practical application

3. Management and Protection of Trade Secret Materials

1) Document Management

(1) Storage

- Documents containing trade secrets must be stored in a locked state in a location inaccessible to anyone except authorized personnel
- If strict storage is difficult due to company size, workplace structure, volume of secrets, or job characteristics, they must at least be separated from general documents and stored in a double-locked cabinet

- Select locking devices appropriately based on security level (ranging from simple locks to advanced security devices)
- Manage separable or detachable records by recording total pages and serial numbers.
- Prohibit overwriting or modification to prevent content alteration

(2) Removal and Duplication

- When authorized personnel remove or duplicate trade secret documents externally, management must be governed by internal regulations
- Removal and duplication are permitted only when necessary for business purposes and require prior approval from the relevant department head (e.g., department manager)
- When copying, clearly mark the original with the date of copying, number of copies, and distribution locations
- Classify copies at the same security level as the original and manage them under the same regulations

(3) Retrieval and Disposal

- Store trade secret documents separately from general documents. Upon completion of use, completely destroy them (to a state where original form cannot be restored and content cannot be recovered)
- Even if copies were made for temporary use, retrieve and dispose of them immediately after use
- Specify the date and time of copying, the number of copies, and the distribution location on the original document when reproducing. - Classify copies at the same level as the original and manage them according to the same regulations

2) Management of Electronic Media

(1) Necessity of Managing the Information Itself

- Electronic data can be massively disseminated in a short time via the internet
- Special attention is required not only for physical storage media but also for managing the intangible information itself

(2) Basic Principles

- Store separately from general information after assigning a management number
- It is advisable to store in access-controlled areas or lockable cabinets

(3) Specific Management Measures

- Establish and adhere to network access rules
- Encrypt email content before transmission
- Establish clear procedures for data replication/backup; backup data must also be encrypted

(4) Management of Authorized Access Personnel

- Set passwords and expiration periods for computer/file access
- Restrict reuse of identical or similar passwords
- Access log monitoring → Enables monitoring of authorized users' access activities to a certain extent

(5) Preventing External Intrusion

- Block third-party intrusion via external networks
- Important to isolate computers handling trade secrets from external networks

(6) Disposal Measures for Equipment

- When disposing of computers or servers storing trade secret data, adhere to the principle of physical destruction
- Electronic records must be completely erased or destroyed

(7) Management of relevant history through security system operation

- Log records of authorized and unauthorized personnel
- Records of data printing and downloading
- Records of file creation, deletion, and modification

3) Restrictions on personal storage media and cloud usage

(1) Prohibition principle

- Prohibition of using personal USB drives, personal email accounts, personal cloud accounts with weak internal security
- Uploading company confidential data to personal storage media or external accounts is prohibited

(2) Exceptional Use

- Personal portable storage devices may be temporarily used only when urgently required for work and with company permission
- After use, data must be returned or destroyed and verified by the security department

4. Computer Management and Communication Security

1) Computer Management

(1) Stored trade secrets are exposed to risk of leakage or theft, requiring caution

- Computers storing trade secrets must implement restricted access and mandatory passwords
- Regularly change passwords on trade secret storage computers to block access by non-authorized personnel

(2) When undergoing external repair or disposal

- Implement measures to prevent data leakage from hard disks

(3) Personal Computers

- Prohibit bringing into or using company premises; if unavoidable, obtain security officer approval before bringing in or out

(4) Research & Development Department/Confidential Storage Computers

- Avoid connecting to external networks whenever possible; if connected, intrusion prevention system operation is mandatory

(5) When Utilizing External Personnel

- Always obtain a confidentiality agreement

2) Communication Security

(1) Due to the constant risk of external eavesdropping on phones, internet, fax, etc., when unavoidable use is necessary

- Encrypt or add/process specific signals before transmission
- Conduct regular and unannounced security inspections of communication facilities; implement corrective measures for deficiencies
- Transmission permitted only after review and approval by the approver designated by internal regulations (department head, security officer, etc.)

(2) E-mail Management

- Set size limits for external outgoing emails
- If the limit is exceeded, department head approval is required before sending
- If possible, set security features like passwords on files before transmission
- Notify the email recipient that the material is important trade secrets
- Impose a confidentiality obligation on the recipient, permitting use of the email content and attachments only within the intended purpose

5. Controlled Area Setup

1) Access Control Devices

- Maintain an access log in controlled areas; enforce access restrictions based on position
- Install advanced surveillance equipment (e.g., CCTV, infrared detectors, RFID) for constant monitoring

2) Regular Access Management

- Require confidentiality agreements from regular access personnel
- Ensure consistent security awareness through these agreements

3) Management of Temporary Visitors

- Maintain and record visitor logs
- Record entries in the trade secret access log

4) Management of External Visitors

- Access permitted only to pre-approved visitors
- Visitors must carry distinctly colored visitor badges from internal staff
- Access to areas posing trade secret disclosure risks is restricted as a rule
- If access is unavoidable, a confidentiality agreement must be obtained

6. Security during Meetings

1) Precautions for External Collaboration and Business Activities

- Verify attendees during in-person or remote video conferences to prevent exposure of trade secrets
- Strictly limit attendance to authorized participants only
- Maintain high-level security during situations with high risk of trade secret leakage, such as third-party consultations or IR (Investor Relations) meetings

-When entering joint research or technology transfer agreements with third parties

→ Always execute a NDA, imposing confidentiality obligations on the counterparty

- During project execution, use only official company email → Prohibit use of personal SNS, etc.

2) Responding to Data Requests from External Parties

(1) Must verify whether the requested materials fall within the scope of purpose defined in the Non-Disclosure Agreement

(2) When providing trade secrets

- Mark PDFs/printed materials as trade secrets or indicate the presence of confidential information in the email body
- Maintain a record by exchanging a Confidentiality Material Provision/Receipt Confirmation

3) Notifying the Other Party of Their Obligations

- Must remind the party receiving trade secrets of their obligation to refrain from using the information for purposes other than those specified and to maintain confidentiality

7. Human Resource Management

1) Designation of Dedicated Security Management Personnel

(1) Necessity of Dedicated Personnel

- Managing trade secrets and company security are mission-critical tasks, making the designation of dedicated staff desirable
- Securing dedicated personnel for trade secret management is ideal; however, if conditions are insufficient, assign a responsible person and delegate management duties
- Dedicated personnel can distinguish and systematically manage trade secrets while also overseeing company-wide security tasks, ensuring continuity, consistency, and expertise

(2) Key Roles of Dedicated Personnel

- Establishment and implementation of trade secret management policies
- Regular audits of internal trade secret management practices
- Gathering and processing employee feedback
- Handling infringement reports, including fact-finding, verification, and evidence preservation

2) Department-Specific Responsible Personnel

- Separate from the dedicated manager, designate department-specific security officers in each department directly handling trade secrets
- Handle specific issues like IT security and access restrictions within the department on-site

3) Security Personnel Deployment

- If feasible, deploy security personnel at company main gates and controlled area entrances
- Enhance security by conducting security checks on visitors

4) Implementation Considerations

- Assigning separate security officers and personnel incurs additional costs
- Implementation decisions and timing should comprehensively consider the company's size, controlled area dimensions, trade secret importance, and financial capacity

5) Alternative Operational Methods

- Until dedicated personnel are assigned, 1-2 employees can concurrently handle security duties
- Utilize security service providers: Outsource security systems, personnel, and inspections

8. Measures to Protect Trade Secrets of Employees upon Resignation

1) Potential for Infringement

- Trade secret infringement occurs most frequently around the time of an employee's resignation
- Inadequate management of departing employees poses risks of difficulty preventing leaks and proving disputes

2) Pre- and Post-Resignation Protective Measures

- Re-obtain non-disclosure agreements
- Enter into non-compete agreements
- Prepare a Confidential Materials/Items Return Confirmation Form
- Preserve digital evidence from electronic devices used by the departing employee
- Conduct an interview with the departing employee

3) Key Content of Departing Employee Interview

- Confirm the career path, new employer, and responsibilities after departure
- Verify the individual's understanding of the confidentiality agreement they signed
- Remind and reaffirm the scope of confidentiality obligations

4) Verify Duties and Contracts

- Verify the departing employee's job responsibilities, assets accessed, and scope of trade secrets
- Review employment contract and confidentiality agreement → Check contractual obligations imposed on the departing employee

5) Security Inspection and Record Management

- Inspect PC usage records up to the time of departure (large downloads, personal email transfers, etc.)
- If violations are found → Request file deletion and verify deletion, document details thoroughly in interview records

6) Digital Evidence Preservation

- Commission digital forensics on the departing employee's electronic devices, obtain expert reports
- Utilize digital evidence preservation services to prevent evidence tampering
- Purpose: Secure intact data evidence in advance to prepare for disputes

How should an exit interview with a departing employee be conducted?	
Preparation	**Consult with the departing employee's direct supervisor and others to confirm the following points in advance**
	- What are the trade secrets in question? (Customer or Technical info?) - Contractual and legal obligations of retirees? (Pledges, employment contracts, etc., signed upon joining or during employment) - Information about the new company, position, and duties at the new company - Whether the departing employee has ever engaged in actions violating company regulations (e.g., email transmissions, etc.)
	Determine who will conduct the exit interview and who will attend
	- Consider the departing employee's personality and relationship with their supervisor - Limit the number of attendees to an appropriate level

Interview	**Confirm the departing employee's obligations and awareness/attitude**
	-Whether they perceive the scope of the duty of confidentiality as excessively narrow or broad -Whether they believe the company's trade secrets have been made public - Whether they believe confidentiality agreements are invalid
	Notify the departing employee of the following matters and obtain their signature, etc.
	- They have received a copy of the non-compete agreement and other contracts -They accurately understand the contract terms, including the confidentiality obligation - They promise to comply with the terms stated in the contract/agreement
Follow-up	**If the retiree displays a negative attitude toward confidentiality, non-compete obligations, etc.**
	- Document the interview with the departing employee in as much detail as possible - Secure relevant evidence such as the departing employee's hard disk drive - Consult with an attorney to consider necessary measures to prevent trade secret infringement (such as filing for a preliminary injunction)

9. Conduct Security Training

1) Necessity of Training

- Confidentiality Agreements signed upon joining the company are often signed without careful review
- As time passes, the contents of the agreement are forgotten, necessitating regular training to raise awareness and enhance understanding

2) Training Objectives

- Ensure employees understand the company's trade secret protection policies and regulations and clearly communicate sanctions for violations
- Enhance practical understanding and compliance awareness regarding trade secret management

3) Training Recipients

- Includes not only employees directly handling trade secrets but all employees and related parties

4) Training Methods

- Can be conducted directly by the security officer
- Can invite external security experts for specialized training when necessary

5) Training Format

- Combine regular and irregular training
- Principle of group training → Also can be replaced with online videos, email material distribution, or internal bulletin board notices depending on circumstances

6) Evidence Management

(1) Evidence must be preserved to document training for dispute preparedness

(2) Methods

- Issue training completion certificates to employees who complete training
- Preserve materials such as event photos and attendance records

10. Remote Work Management Factors

1) Background and Necessity

- Post-COVID pandemic, contactless digital-based work (remote work) has proliferated → Established as a standard work model
- Remote work utilizes personal PCs, laptops, external storage devices, cloud services, etc. outside corporate security networks → Increased risk of information leakage
- Allowing remote work means data may be exposed to an environment where access by non-employees is possible
- Courts of Republic of Korea prioritize whether companies demonstrated a commitment to confidentiality and objective efforts when assessing trade secret protection
- Therefore, companies must supplement existing management methods to align with changing work patterns and document efforts to protect trade secrets

2) Management Guidelines

(1) Establish Remote Work Security Regulations

- Existing office-based regulations have limitations → New security regulations tailored to remote work environments are necessary

(2) Manage Access and Usage Data Lists

- Verify lists of trade secrets and key assets accessed during remote work periods
- Grant access permissions only to the minimum necessary extent
- If access to unauthorized data is required → Permission must be granted only after approval by the department head and security officer
- When using company-shared cloud services → Configure settings to track records of viewing or downloading confidential data by unauthorized individuals, and conduct regular inspections
- Limit the scope of confidential data required for remote work to avoid unnecessary expansion

(3) Establish a Security Inspection System

- Create security checklists tailored to each remote work format to verify appropriate security readiness for implementation
- Mandatorily provide remote workers with work devices equipped with security systems and maintain a management log tracking each user's device serial number and IP address

3) Imposing Confidentiality Obligations on Remote Workers

(1) Need for Differentiation by Job Role

- The scope of trade secrets a remote worker can handle varies based on their assigned job role and position
- Employees directly handling trade secrets, and those in positions of greater responsibility, require stricter obligations

(2) Security Pledge Agreement

- Require remote work approval recipients to sign a remote work security agreement
- Specify concrete confidentiality obligations in the agreement

(3) Work Authorization and Sanctions

- Decide remote work approval based on the applicant's job position and impose strict sanctions, such as restricting remote work types

4) Verify Security Suitability of Remote Work Location Facilities

(1) Scope of Work Locations

- Scope of remote work locations and restrictions on changes vary by company policy
- Some companies impose minimal restrictions on frequent changes to remote workers' locations

(2) Restrictions by Job Characteristics

- Restrictions on permissible work locations are necessary based on the nature and importance of the work performed by remote workers
- Employees handling core trade secrets or with high access frequency must work only in locations meeting minimum security standards

(3) Security Verification Procedures

- Companies require remote work applicants to submit supporting documents such as site verification forms for confirmation
- After reviewing submitted materials, if deemed inadequate for security, instruct the employee to work from a security-compliant location

5) Requirement for Remote Workers to Complete Security Self-Checklists

(1) Obligation to Complete Self-Checklists

- Remote workers must complete security self-checklists to understand essential security requirements
- The checklist must be completed before and during remote work to ensure self-awareness of security precautions

(2) Company Responsibilities

- The company must provide the self-check form template and post a brief explanation
- This ensures adequate notification of key security requirements to remote workers

[Table 5] Application for remote work arrangement

APPLICATION FOR REMOTE WORK ARRANGEMENT

1. Application

Last Name	First Name	Initial
Address		
		Postal Code
Department	Division	Section
Classification/Working Title		Position Number
Employee Number		Phone # (work)

2. Dates

Period of remote work being requested:

FROM (dd / mm / yy) ____ / ____ / ____ TO (dd / mm / yy) ____ / ____ / ____

Please specify the start time and end time:

	Monday	Tuesday	Wednesday	Thursday	Friday	Total
Designated Work Site						
Remote work						
Total Hrs/day						

% of time at the Designated Work Site: _____
% of time at the Remote Work Site:

3. Reason for request

_____
_____
_____
_____
_____

4. Employee Signature

_____	_____
Date	Employee

I hereby agree to this employee's application, pending meeting the requirements as outlined in the Remote Work Guidelines and Agreement.

_____	_____
Date	Supervisor/manager
_____	_____
Date	Human Resource Manager
_____	_____
Date	Deputy Head/Director

[Table 6] Remote work agreement

PROVINCE OF PRINCE EDWARD ISLAND

REMOTE WORK AGREEMENT

_____
(the Employee)

AND

_____
(the Employer)

The Employer and the Employee agree as follows:

Schedule

1. (a) The Employee's normal work week will consist of:
   (ⅰ) _____as designated work site days.
   (ⅱ) _____as remote work site days.
   (b) Subject to amendment or termination by the Employer at its discretion Or in the form of a written request from the employee;

2. Daily hours of work shall be:

_____

Employee

3. The employee's status, eligibility for authorized overtime, obligations, benefits and entitlements are not altered by this Agreement. Overtime wherever possible should be pre-authorized by the Employer.

Home Office

4. The Remote Work site location of the Employee is:

Remote work Site Address: _____

_____

Phone/Email: _____

Home Renovations	5. Except as provided in paragraph 18, the Employee is responsible for all costs associated with home renovations and/or electrical upgrades Required for a remote work site.
Safety	6. The Employee agrees to maintain a designated workspace that meets the Employer's normal workplace occupational health and safety standards for the remote work site. A visit may be made by the Manager or Supervisor and PSC OHS section staff to review health and safety issues on reasonable notice to the Employee.
	7. The Employee agrees to promptly report all work-related incidents and accidents to the Supervisor or Manager.
	8. Clients are not to be seen in the remote work site for liability reasons.
On-Site on-**Visits**	9. The Employee agrees to make the remote work site accessible for site visits by Employer representatives for safety inspections, accident investigation, security and equipment audits and other work related matters.
Insurance	10. The Employee agrees to carry USD 2,000,000 of general liability insurance, and costs associated with this coverage are the responsibility of the employee. The Employee is responsible to advise their insurance company of the remote work arrangement, and provide confirmation of adequate coverage, to the Employer.
	11. The insurance coverage does not extend to equipment and furniture owned by the employee.
Family Responsibilities	12. The Employee agrees to have arrangements in place for regular dependent care.
Equipment	13. The Employer will provide equipment as follows: Item: _____ Serial#_____ _____ _____
Security	14. The employee must sign an Acceptable Use Policy for Computer Systems and VPN Request form. The Employee must ensure that required IT security standards are followed at all times. A dedicated LAN connection or a password protected wireless connection must be used.

Technical Support	15. ITSS will provide the service necessary for the installation, upgrading, maintenance and removal of hardware, software, virus protection and peripheral equipment. Service will be provided remotely when possible, or may require the employee to bring the device to a designated location.
Costs/ Expenses	16. The Employer will supply or pay for the following costs and service charges associated with the remote work site (e.g., office supplies, courier, and work related telephone expenses). _____
	17. All remote work site-related expenses must be pre-authorized and supported by receipts.
	18. The Employer is not responsible for any costs not specified in this agreement.
Travel	19. The Employee is eligible for travel expenses as outlined in the Treasury Board Policy Manual.
	20. The Employee is responsible for any costs associated with travel to the designated work site, including trips to and from the designated work site, on any of the remote work site work days.
Amendment	21. Withdrawal from the program or any revisions requested is required to be in writing to the Employer.
	22. Notwithstanding clause 21, this agreement automatically terminates when the employee moves to a new position.
Additional Conditions (as agreed to by employee and manager/ supervisor)	23. _____ _____

Date	Employee
_____	_____
Date	Manager or Supervisor
_____	_____
Date	Deputy Head/Director

Origianl-Employee Personnel file **Copy-Employee** **Copy-Manager or Supervisor**

[Table 7] Remote access Confidentiality and Security Agreement

REMOTE ACCESS CONFIDENTIALITY AND SECURITY AGREEMENT

I understand and agree that, in the performance of my duties as an employee, physician or agent of [company], I have been granted remote access to some of the Medical Center's computerized information systems. As a condition of this access, I understand and agree to the following requirements:

I will not divulge or make known to any other person, either the password or the unique security code that is assigned to me for access to the Medical Center's information systems. I will also not use or attempt to use any other password or security code to access data in the Medical Center's information systems other than those authorized and assigned to me by the Medical Center. If I have reason to believe that my security code is known by someone else, I will notify the Medical Center's designated representative immediately for assignment of a new code.

I will access the Medical Center's information systems in the manner designated by the Medical Center. I will not leave my computer unattended while still connected in a remote session. When finished with a remote session I will promptly log off the system and end the connection.

I will not discuss any information, status, treatment or condition of any Medical Center patient with anyone, including another employee, physician or agent of the Medical Center, in a place or in a manner which may compromise the confidential nature of the information being provided from the Medical Center's information systems.

I agree to hold the Medical Center harmless from and against any and all claims, liabilities, costs, expenses and damages arising out of or in connection with my failure to adhere to the above conditions.

I understand the above conditions and agree that violation of any of these conditions will result in appropriate disciplinary actions, which may include termination of my employment with the Medical Center.

WVC number_____

Print Name Date

Signature

[Table 8] Remote Work Security Checklist (For Supervisor)

Remote Worker Agreement Supervisor Checklist

Supervisors must use this checklist to ensure that remote work requirements are met and that covered employees understand the policies and procedures of the remote work program. A Remote Worker Agreement is not final until the checklist is complete. After an item is completed, list the date on the line next to it.

Checklist Item:	Date Completed:
1. Remote Guidelines have been explained to the employee and signed by supervisor and employee (attached).	
2. The provisions governing premium pay have been explained to the employee including that he/she must receive the supervisor's approval in advance of working overtime.	
3. Performance expectations have been discussed with the employee. Performance Standards are in place and have been signed.	
4. Policies and procedures covering classified, secure and privacy data including PII have been explained to the employee.	
5. The provisions governing changes to the terms and conditions of the remote work agreement have been explained to the employee, including that they must receive the supervisor's approval in advance of any changes to the location of the duty station (i.e., remote work site). Failure to obtain management approval may result in termination of the remote work agreement.	
6. The employee has been given and signed the Safety Checklist, which identifies safety and adequacy issues that employees should consider when working from home (attached).	

Also, identify any equipment/property that will be provided for the remote site below, as applicable:

Item	Yes	No
Computer:		
Docking Station:		
Printer:		
Monitor:		
Keyboard:		
Mouse:		
Other Item1:		
Other Item2:		
Other Item3:		
Other Item4:		

11. Evidence Preservation for Trade Secret Management

1) Purpose of Preservation

(1) In trade secret infringement cases in Republic of Korea, it is required to prove not only the act of infringement itself but also the following factors

- The specification and scope of the information claimed as a trade secret
- Whether the information satisfies the requirements of non-publicity, economic value, and secrecy management
- Whether the information belongs to the affected company

(2) To this end, companies must secure and preserve materials capable of proving the facts and timing of management

2) Examples of Materials to Preserve

- Confidentiality agreements/undertakings
- Certificates of completion for security/trade secret training
- Access logs for secure areas
- Trade secret registers and ledgers
- Records of authorized access permissions for trade secrets

3) Management Method

- Department heads and trade secret management officers must separately store relevant materials

4) Utilization of External Systems

(1) Original Document Certification Service (operated by Korea Intellectual Property Information Service Trade Secret Protection Center)

- Enables public certification of facts such as the trade secret's attribution to the company and the time of possession

(2) Purpose of the Original Proof System

- Enhance the convenience of proving ownership for trade secret holders
- Electronic documents containing trade secrets must receive originality certification from designated institution

3. Developing a Business Intellectual Property Portfolio

Introduction

Understanding the complementary roles of patents and trade secrets is essential for building an effective technology protection strategy. As innovation accelerates and information leakage risks grow, companies must evaluate the characteristics of their technologies to select appropriate protection methods or hybrid approaches.

Patents provide strong exclusive rights for inventions that meet legal requirements but require full disclosure and entail costs and strategic risks. They are most effective when reverse engineering is easy or infringement is easily detectable.

Trade secrets cover a broader range of technical and business information without disclosure or time limits, but they do not provide exclusive rights and cannot prevent independent development or reverse engineering.

Choosing the appropriate protection mechanism requires assessing the nature of the technology, risk of imitation, lifecycle, competitive environment, and business goals. In some cases, auxiliary legal systems, such as design protection or unfair competition laws, may offer additional options.

The most effective approach is typically a ‘multi-layered portfolio strategy’, combining patents and trade secrets to maximize protection, support commercialization, and enhance long-term competitiveness.

This section explains the characteristics of patents and trade secrets and presents a general business IP portfolio.

As the systems and operational methods of each economy differ in this regard, this guidebook focuses on elements that can be referenced in general terms. It is recommended that the detailed application methods and system design be flexibly supplemented and developed to suit the policy and organizational conditions of each member economy.

I. Understanding Patent and Trade Secret Protection Systems

1. Patent: The Need for Trade Secret Protection Strategies

1) Intensifying Global Technology Competition and the Need for Technology Protection
   - Increased importance of protecting corporate core technologies amid intensifying global technological competition
   - Protecting technologies secured through R&D using appropriate intellectual property means is key to maintaining corporate competitiveness
   - Companies face the decision of whether to protect their technology through patents or trade secrets
   - Technology leakage has a significant adverse impact not only on corporate survival but also on the internal economy
2) Limitations of Patent Protection Alone
   - Patents require mandatory disclosure of technology → Risk of unnecessary information exposure
   - Relying solely on patents without strategy risks providing core information to competitors
3) Limitations of Trade Secret Protection Alone
   - Once a product enters the market, competitors can reverse-engineer and analyze it
   - If competitors imitate or improve upon it and secure patents first, the original technology holder may face restrictions on its own use
4) The Need for a Multi-Layered Technology Protection Strategy
   - Requires a multi-layered protection system combining patents and trade secrets based on technology characteristics
   - Selection must comprehensively consider the technology's nature, lifecycle, industry structure, reverse engineering potential, etc.
   - The most effective approach is the complementary use of patents and trade secrets

2. Definitions

1) Definition of Patent

(1) Basic Concepts

- Patent law protects 'inventions'
- Invention: A highly creative technical idea utilizing natural laws
- Satisfies requirements of industrial applicability, novelty, and inventive step

→ Grants exclusive rights in exchange for public disclosure of the technology

(2) Characteristics of the Protection Method

- Ability to exercise exclusive rights for a fixed period (maximum 20 years)
- Civil and criminal remedies available for infringement
- Strict requirements for establishment, but strong rights after registration

(3) Subject Matter of Protection (Types of Inventions)

- Product Inventions: Components, products, devices, materials, substances, etc.
- Method Inventions: Production/manufacturing methods, usage methods, etc.

2) Definition of Trade Secrets

(1) Basic Concept

① Technical or business information is protected when it meets the following requirements

- Non-publicity, Economic usefulness, Proprietary Management

② Protection for managing the information itself in a confidential state (not in the form of exclusive rights)

(2) Characteristics of the Protection Method

① No registration procedure → Relaxed requirements for establishment

② Protection possible for both technical information and business management Information

③ Absence of monopoly or exclusive rights

- Cannot prohibit third parties from independently developing the same technology
- Use restrictions may arise if competitors obtain patents for identical technology

(3) Scope of Protection

- Technical trade secrets

Subject	Description
Facility and product design drawings	Design drawings for critical factories, layout diagrams for machinery and equipment, design drawings for product production lines, process design drawings
Production of Goods	Product production, processing, assembly, or manufacturing methods that are proprietary or undisclosed
Method of Combining Substances	Reaction sequences for material creation, raw material blending sequences, blending ratios, timing differences, etc., that are undisclosed and cannot be reverse engineered
Research and development reports and data	Research and development process, results report, and data used in the research
Experimental data	Performance testing of prototypes under development or prototype prototypes, efficacy of pharmaceuticals, commissioning data for machinery and equipment, etc.
Facilities, machinery, and equipment	Facilities, specialized equipment, and installations independently developed and owned by a company or individual equipment

-Business trade secrets

Subject	Description
Various key plans	Management strategy, new investment plans, new product development· Production plans, marketing· Sales plans, workforce supply plans, etc.
Customer Lists	Regional customer lists, age-based or occupation-based classification tables, and agency· sales office sales materials, etc.
Management Information	Cost analysis, margin rates, business partner information, personnel· financial management and business analysis information, etc.
Manuals and other critical documents	Methodology documents based on the company's technology and experience, manuals containing unique methods or techniques specific to the company

3. Differences and Advantages/Disadvantages between Patents and Trade Secrets

1) Fundamental Differences between the Two Systems

(1) Subject of Protection

① Patents

- Protection of technical ideas and the technology itself

② Trade Secrets

-Protects technical information (know-how) and business management information

(2) Requirements for Protection

① Patent

- Must satisfy novelty, inventive step, and industrial applicability

② Trade Secrets

- Must satisfy non-publicity, secrecy management, and economic usefulness

(3) Disclosure Status

① Patent

- Disclosure of technology after patent application or registration

② Trade Secrets

- Maintain non-disclosure

(4) Protection Procedures· Duration· Cost Differences

① Patent

- Requires the procedure: Application → Examination → Registration
- Cost burden exists
- Up to 20 years of protection from the filing date

② Trade Secrets

- No separate application required· No examination· No registration procedure required
- No limitation on protection period as long as secrecy is maintained

(5) Exclusivity: Existence of Exclusive Rights

① Patent

- Strong monopoly· exclusive rights exercised during the term (max 20 years)
- Patent infringement occurs even if competitors independently develop the same technology
- Can claim injunctions, damages· , and even criminal liability against infringers

② Trade Secrets

- No exclusive rights
- No infringement if third party independently develops identical technology or acquires it through reverse engineering· analysis, etc.
- In such cases, injunction· and damages claims are not possible
-Transfer: Implementation agreements may be concluded, but it is not a proprietary exclusive right; registration is also impossible

(6) Remedies for Infringement

① Patent

- Civil and criminal actions possible under the Patent Act

② Trade Secrets

- Protected based on contract terms; also governed by the Unfair Competition Prevention Act, the Trade Secrets Protection Act, the Act on the Prevention of Leakage and Protection of Industrial Technology, etc.

Classification	Patent	Trade Secrets
Subject	Technology (technical ideas, the technology itself)	Technical Information (Know-how), Business Information
Protection Requirements	Novelty, Inventive Step, Industrial Applicability	Non-publicity, confidentiality management, economic usefulness
Disclosure of Technology	After patent application or registration, Disclosure of Technology	Non-disclosure
Procedure	File a patent application with the Patent Office, undergo examination by an examiner, and proceed with patent registration	No separate procedures required at offices for application, examination, registration, etc. No need for separate procedures at other agencies
Term of Protection	20 years from the patent application date	No time limit (Protected indefinitely if kept confidential)
Cost	Patent application and registration, and maintenance fees required	No direct costs required
Enforcement	Exclusively exercise rights (Patent infringement is established even if developed independently later)	No exclusivity (Subsequent independent development, reverse engineering· analysis, etc. no trade secret infringement occurs)

Classification	Patent	Trade Secrets
Remedies for Infringement	Civil and criminal remedies available under the Patent Act Protection under contract terms	Protected by contract terms; Unfair Competition Prevention and Trade Secret Protection Act, Industrial Technology Leakage Prevention and Protection Act, etc.

2) Comparison of Advantages and Disadvantages

(1) Advantages of Patents

- Strong monopoly
- Potential for revenue generation through licensing
- Competitors' independent development of identical technology can be sanctioned as infringement
- Advantageous when the invention's content is easily discernible (e.g., through reverse engineering) or when product commercialization makes proving component infringement straightforward
- Civil and criminal remedies available against infringers

(2) Advantages of Trade Secrets

- No limitation on protection period while maintained as a secret
- Protects a wider and more comprehensive range of subject matter than patents
- No need for disclosure → Core know-how can be concealed
- When disclosed alongside processes, software, etc., easier for third parties to imitate
- More advantageous than patents when proving infringement is difficult

(3) Disadvantages of Patents

- Patent disclosure → Risk of imitation· and improvement
- Cost burden exists during the registration process
- Limited protection period (maximum 20 years)

(4) Disadvantages of Trade Secrets

- Protection impossible if third parties can independently develop· reverse engineer it (difficulty prohibiting third-party use), unless trade secrets were improperly obtained
- Difficulty enforcing rights in case of disputes

Cat.	Patent	Trade Secret
Pros	- Securing exclusive rights - Potential for generating income through licensing - Competitors' independent development of identical technology can be considered infringement and subject to sanctions - Patents are advantageous when the invention's content is easily discernible through reverse engineering or when commercialized products make it easy to prove infringement of specific components - Civil and criminal remedies available against infringers	- No limitation on protection period as long as it is managed confidentially - Trade secrets cover a broader and more comprehensive range than patent rights - Core know-how can be concealed by not disclosing it - Trade secrets are advantageous when the subject matter (e.g., processes like mechanical process technology or chemical manufacturing technology, or software like algorithms) is easily imitated by third parties upon disclosure and infringement is difficult to prove
Cons	- In principle, all patents are disclosed, enabling third parties to imitate or improve upon inventions and secure rights to them - Costs must be borne during the registration process. - Upon expiration of the patent term (20 years), anyone may use the invention	- If confidentiality management fails, it is difficult to prohibit third-party use unless it constitutes misappropriation of trade secrets - Difficulty in enforcing rights when disputes arise

3) Comprehensive Implications

- Trade secrets appear advantageous over patents in terms of procedure, cost, and duration, but lack of exclusivity means they cannot counter competitors' independent development or reverse engineering
- Patents carry disclosure burdens and registration constraints, but once registered, they become the strongest means of technological protection
- Therefore, companies must comprehensively evaluate the pros and cons of patents and trade secrets, considering factors like technological characteristics, reverse engineering risks, and competitive environments. A parallel or hybrid strategy is preferable over relying on a single approach

II. Multi-Layered Portfolio Strategy

1. General Information

1) The Need for a Technology Protection Strategy

(1) Distinguishing Technical Information from Business Information

- Need to choose whether to protect technical information by disclosing it via patents or by maintaining secrecy
- Business information cannot be protected by patents, making trade secret protection essential

(2) Importance of Selection

- Disclosing technology enables competitors to imitate it
- Keeping it confidential makes it vulnerable to reverse engineering or independent development
- The choice of protection method based on the technology's characteristics directly impacts a company's competitiveness

(3) Considerations

- Type and lifespan of the technology
- Industry demand
- Existence of competing technologies
- Difficulty of detecting and proving infringement

2) Criteria for Choosing Between Patents and Trade Secrets

(1) Representative Criteria

① Whether the technology is protectable by patent or trade secret

② Possibility of reverse engineering and analysis

③ Ease of detecting and proving infringement

④ Potential for technology transfer, investment attraction, and marketing utilization

⑤ The company's technological level and R&D strategy

(2) The Complex Nature of Judgment Criteria

- Some criteria recommend selecting patents
- Other criteria support trade secret selection

→ Comprehensive evaluation of each criterion is necessary to select the optimal means of protection

3) Procedure for Reviewing Protect-ability and Satisfaction of Requirements

(1) Step-by-Step Structure for Selecting Protection Measures

① Confirm eligibility for protection

- Patent: Must qualify as an 'invention'
- Trade secrets: Must qualify as 'technical or business information'

② Review of Protection Requirements

- Patent Requirements: Industrial applicability, novelty, inventive step
- Trade secret requirements: Economic usefulness, non-publicity, secrecy management

③ Select patent or trade secret based on technical characteristics and competitive landscape

(2) Alternative Protection Methods

- If neither patent nor trade secret is feasible

→ Protection possible via Design, Protection Act, Trademark Act, Unfair Competition Prevention Act, etc.

4) General Selection Process and Practical Considerations

(1) When a patent is advantageous

- Technology susceptible to reverse engineering
- Technology with high likelihood of competitor imitation
- Core technology scheduled for commercialization
- Technology where infringement is relatively easy to prove

(2) When trade secrets are advantageous

- Cases where disclosure poses significant risks, such as processes or algorithms
- Technologies where reverse engineering is difficult and internal know-how is critical
- Technologies capable of long-term confidentiality

(3) Practical implications

- If trade secrets are chosen, managing confidentiality is critical
- Design technology protection strategies from the product development stage to minimize risk

5) Key Points

- Comprehensive review of technology-specific characteristics, risks, and market conditions is necessary
- Rather than choosing either patents or trade secrets alone
  → An "appropriate combination or hybrid strategy" can be the optimal means of technology protection
- Companies must establish technology protection strategies in advance and continuously update them in alignment with business and R&D strategies

2. Protection Strategy Points

Protection Strategy Point 1	<Device/Element/Material/Composition/Substance> Protecting tangible items via patents is generally advantageous

- Where reverse engineering can reveal the structure or material composition, or where component analysis is possible, the technology should be protected through patent rights
- Upon patent registration, exclusive rights such as injunctions against infringement and claims for damages can be exercised against competitors' implementations falling within the scope of the rights
- Even if registration is not achieved, disclosure can prevent similar technologies from being patented
- For technologies undergoing continuous R&D or those nearing commercialization, it is advisable to build a robust protection barrier through multiple patent applications to provide thick protection

Protection Strategy Point 2	<Processes, Algorithms> When the substance is difficult to grasp easily, protecting it as a trade secret is advantageous

- When filing a patent application for a process or algorithm, disclosure occurs 1 year and 6 months after the filing date. Therefore, it is essential to carefully assess whether filing

a patent application is preferable or if protecting it as a trade secret is more advantageous

- If disclosure occurs, protecting core process or algorithm technologies as trade secrets may be advantageous, as competitors could otherwise understand and improve upon the technology
- Even if a patent application for a process or algorithm is filed and granted, proving that a competitor's implementation infringes the patent's scope of rights is often extremely difficult, making enforcement challenging
- However, when protecting as a trade secret, it must be managed with strict confidentiality to prevent leaks

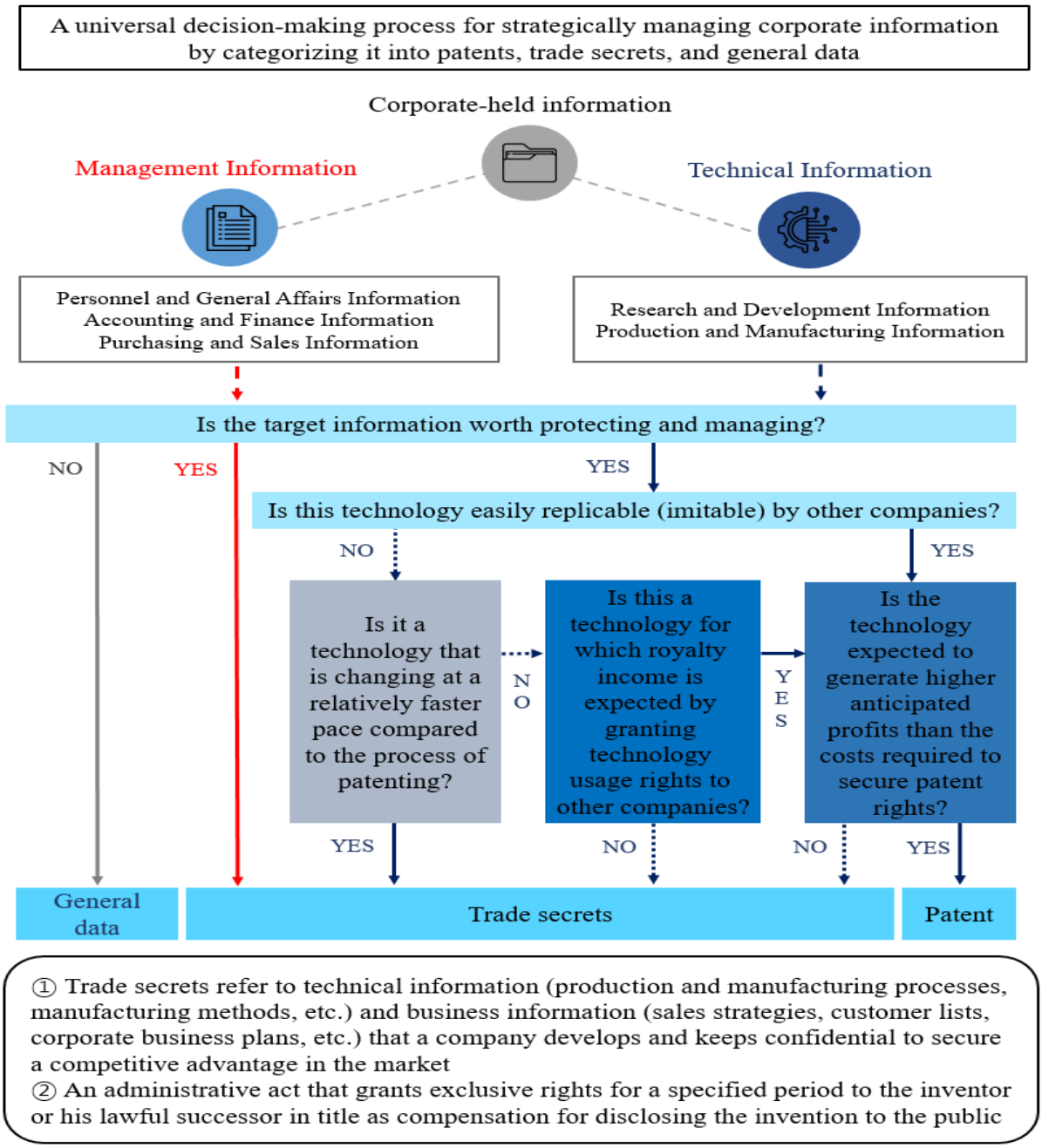
Protection Strategy Point 3	<Intensifying Competition, Ease of Imitation> Choose between patent application and trade secret management based on the situation

- When multiple companies are positioned in the same technological field, making competition extremely fierce, patent application may be advantageous in some cases, while managing as a trade secret may be advantageous in others
- For significantly advanced technologies, patent applications may be advantageous. Protecting various aspects through patents can establish a patent barrier, enabling differentiation from competitors
- If the technology developed by the company is very straightforward, managing it as a trade secret to prevent exposure can secure competitiveness
- If the developed technology can be easily imitated once the product is launched, securing patent rights is necessary to enforce against competitors' imitations
- If the technology field where the company's technology resides has frequent disputes, acquiring patent rights is advantageous for responding to disputes

Protection Strategy Point 4	<Depending on the Purpose> If the purpose is technology transfer, collateral loans, or marketing, prioritize reviewing patent applications

- If the purpose is technology transfer or IP-backed loans, acquiring patent rights is advantageous
- If the purpose is marketing, proceeding with a patent application is advisable. The examination request period (3 years from the filing date) can be appropriately utilized

[Figure 1] multi-layered portfolio strategy process



- The red line means management information, while the blue line means technical information

- The selection process for protection methods may vary by expert opinion and is not an absolute standard

* Excerpt from 'Trade Secret Protection System: The Cornerstone of Technology Protection'

[Appendix]

Trade Secret Protection Systems in APEC Member Economies

Australia

Legal Framework

□ **Legal Basis:**

- No standalone statute governing trade secrets
- Protection grounded in common law, especially via confidentiality agreements

□ **Legal Concept:**

- "Trade secrets" not legally defined
- Aligned with "undisclosed information" under the TRIPS Agreement

□ **Corporations Act 2001:**

- Imposes confidentiality obligations on company officers and employees
- Prohibits improper use of information obtained through one's position

□ **Privacy Act 1988:**

- Allows the Privacy Commissioner to address unfair disclosure of sensitive business information

□ **Freedom of Information Act 1982:**

- Enables agencies to refuse disclosure of documents if it would breach confidentiality

Civil Remedies

□ **Civil Claims:** Available under general limitation rules for trade secret

□ **Limitation Period:** 6 years (most jurisdictions) / 3 years (Northern Territory)

□ **Remedies:** Equitable compensation to restore injured party's position

□ **Punitive damages:** Not typical; allowed for copyright or contract breach

Criminal Remedies

□ **Legal Basis:** Section 184 of the Corporations Act 2001

□ **Scope:** Criminal liability applies to misuse of confidential information by officers or employees

□ **Intentional misuse:** Using information dishonestly to gain an advantage or harm the company

□ **Reckless misuse:** Using information recklessly in a way that may cause such outcomes

Case

□ *In Smith Kline and French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health* — A leading case establishing that, unlike general information, confidential information must possess specific identifiability to be recognized as confidential information.

Business Support Program for MSMEs

□ Australia does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for SMEs, as the protection of trade secrets is primarily governed through general legal principles rather than a standalone statutory framework

Brunei Darussalam

Legal Framework

□ **Legal Basis:**

- No legislation specifically governing trade secrets
- Official Secrets Act applies only to public security, not private sector trade secrets

□ **Judicial Reference:** UK case law used as persuasive authority in courts of Brunei Darussalam

□ **Elements of Breach:**

- Information is inherently confidential
- Recipient had an obligation to maintain confidentiality (objectively assessed)
- Breach occurred through unauthorized disclosure or use

□ **Non-Contractual Protection:**

- Claims possible even without a contract
- Applies if recipient knew or should have known the information was confidential

□ **Contractual Protection:**

- Secured through employment contracts or NDAs
- Obligations may continue after termination

□ **Drafting Guidance:**

- Confidentiality clauses must be clear and explicit for enforceability

Civil Remedies

□ **Legal Basis:** No statutory civil remedies specific to trade secrets

- Breach of contract claims possible if trade secrets are contractually protected
- Damages for losses, or equitable remedies like injunctions and account of profits
- All remedies are grounded in common law, not statute

Criminal Remedies

□ **Legal Basis:** No statutory framework for trade secrets, and no criminal sanctions apply to their misappropriation

Business Support Program for MSMEs

□ Brunei Darussalam does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for small and medium-sized enterprises

□ Nevertheless, the Economic Development Board of Brunei Darussalam offers comprehensive business process support services to assist companies

□ For more information, please refer to :

https://www.bedb.gov.bn/business-support

Canada

Legal Framework

□ **Legal Basis:**

- No legislation specifically governing trade secrets
- Civil protection through common law (e.g., contract law, duty of good faith)
- Criminal definition and protection under Section 391 of the Criminal Code

□ **Practical Protection Mechanisms:**

- Internal policies, employee access controls, and information management systems
- Use of NDAs and confidentiality clauses in contracts
- Physical, technical, and administrative safeguards

□ **Statutory Definition:**

- Section 391(5) of the Criminal Code defines "trade secret" as information that:
- Is not generally known in the trade or business
- Has economic value due to its secrecy
- Is subject to reasonable efforts to maintain secrecy

□ **Global Alignment:**

- Legal definition aligned with global standards (e.g., TRIPS Agreement)
- Three-pronged test: secrecy / economical value / reasonable protection efforts

Civil Remedies

□ **Legal Basis:**

- Grounded in common law (not statute)
- Claims based on breach of contract, fiduciary duty, unjust enrichment, or unlawful interference

□ **Relief Available:**

- Damages (compensatory or account of profits)
- Equitable remedies such as injunctions

□ **Factors Considered by Courts:**

- Efforts to maintain secrecy
- Value and development cost of the information
- Ease of independent acquisition
- Owner's and recipient's treatment of the information as confidential
- Whether recipient should have known it was confidential
- Whether misuse caused harm to the owner

Criminal Remedies

□ **Legal Basis:**

- Section 391 of the Criminal Code (R.S.C., 1985, c. C-46)
- Provides statutory definition of "trade secret"
- Establishes criminal liability for improper acquisition and use

□ **Primary Offense (391(1)):**

- Knowingly acquiring trade secrets through deceit, falsehood, or fraud
- Disclosing or making the secret accessible to others without authorization
- Extends liability beyond acquisition to include unauthorized sharing

□ **Secondary Offense (391(2)):**

- Acquiring or disclosing trade secrets knowing they were obtained through an offense
- Includes situations where the person is willfully blind to the unlawful origin
- Targets downstream distribution and continued misuse

□ **Penalties (391(3)):**

- Indictment: up to 14 years' imprisonment
- Summary conviction: lesser penalty for minor cases
- Reflects proportionality in enforcement based on case severity

□ **Exception (391(4)):**

- No criminal liability for reverse engineering
- No criminal liability for independent development
- Protects legitimate innovation and fair competition practices

□ **Legislative Purpose and Policy Rationale:**

- Addresses both direct misappropriation and downstream misuse
- Aims to protect confidential business assets and promote fair competition

Case

□ *Cadbury Schweppes Inc. v. FBI Foods Ltd* — A case addressing trade secret infringement, breach of a relationship of trust, the constituent elements and protection requirements of trade secrets, and the scope of available remedies

Business Support Program for MSMEs

□ Canada does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for small and medium-sized enterprises.

Chile

Legal Framework

□ **Legal Basis:** Governed by Industrial Property Law (Ch. VIII) and Criminal Code

□ **Definition of Art. 86:** Undisclosed, economically valuable, and protected by reasonable measures

□ **Legal Criteria:** Secrecy / Economical value / Confidentiality efforts

□ Misappropriation (Art. 87): Unauthorized use or disclosure; breach of duty with intent to benefit or harm

□ **Secrecy Scope:** Not generally known or accessible; includes non-obvious combinations

□ **Protection Measures:** Limited access, NDAs, internal confidentiality procedures

Civil Remedies

□ **Legal Basis:** Article 88 of the Industrial Property Law; remedies under Title X

□ **Available Remedies:**

- When industrial property rights are infringed or affected, the right holder may request legal remedies
- Injunction to stop misappropriation, monetary damages, preventive measures, publication of ruling at infringer's expense

□ **Damages Assessment Methods:**

- Lost profits of the claimant
- Gains obtained by the infringer
- Reasonable royalty under a hypothetical license

□ **Exception:** No liability for sellers unaware of infringement at time of sale

Criminal Remedies

□ **Legal Basis:** Industrial Property Law Art. 88; Criminal Code Arts. 284–284ter

□ **Offenses:** Unauthorized access, disclosure, or use of trade secrets

□ **Scope:** Includes breach of trust, technical intrusion, and use with knowledge of illicit origin

□ **Penalties:** Imprisonment with harsher penalties for third-party disclosure

Business Support Program for MSMEs

□ Chile does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for small and medium-sized enterprises

People's Republic of China

Legal Framework

□ **Legal Basis:**

- The 「*Anti-Unfair Competition Law of the PCR, AUCL*」
- Supplemented by Civil Code, Criminal Law, Labor Contract Law, Company Law, Civil Procedure Law, and Technology Achievement Law

□ **Definition of Trade Secrets (AUCL, Article 10):** Non-public technical or business info with economical value, protected by confidentiality measures

□ **Types of Misappropriation Include:**

- Acquiring trade secrets via theft, bribery, fraud, coercion, electronic intrusion, etc.
- Disclosing or using improperly obtained secrets, or enabling others to use them
- Breaching confidentiality obligations or requirements, disclosing, using or allowing others to use trade secrets.
- Inducing/assisting third parties to breach confidentiality, obtaining, disclosing, using or allowing others to use the right holder's trade secrets.

Civil Remedies

□ **Available Civil Remedies:** Injunctions and monetary damages

□ **Evidence:**

- Civil litigation for trade secret infringement follows the principle of "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.
- If the claimant provides preliminary evidence proving that it has taken confidentiality measures for the claimed trade secrets, and reasonably indicates that the trade secrets have been infringed, the defendant shall prove that the trade secrets claimed by the right holder do not meet the constitutive elements of trade secrets;
- If the claimant provides preliminary evidence reasonably indicating infringement of trade secrets and provides any of the following evidence, the defendant shall prove that it has not infringed the trade secrets: (i) evidence that the defendant had access to or opportunity to obtain the trade secrets, and the information it used is substantially identical to the trade secrets; (ii) evidence that the trade secrets have been disclosed, used, or there is a risk of disclosure or use; (iii) other evidence that the trade secrets have been infringed.

□ **Statute of Limitations:**

- Starts when the right holder knows/should know of the infringement of the right and the person who owes the obligation
- The general statute of limitations period is three years. If twenty years have passed since the date of infringement, the People's Court shall no longer provide protection for 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:**

- Based on actual losses suffered by the right holder
- If not measurable, based on the benefits obtained by infringer from the infringement
- Reasonable enforcement costs are also recoverable

Criminal Remedies

□ **Legal Basis:** Article 219 and Article 219(1) of the Criminal Law

□ **Offenses constituting the crime of infringing trade secrets includes:**

-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 the trade secrets obtained by means mentioned in the preceding item;
- Disclosing, using, or allowing others to use the trade secrets it possesses, in violation of its confidentiality obligation or the right holder's requirements for keeping the trade secrets confidential.
- Whoever knowingly obtains, discloses, uses, or allows others to use the trade secrets as described in the preceding paragraph shall be deemed to have infringed the trade secrets.

□ **Penalties:**

- In serious cases, imprisonment for up to three years or a fine
- In particularly serious cases, imprisonment for not less than three years and not more than ten years, along with a fine

□ **Offenses constituting the crime of stealing, spying, buying, or illegally providing trade secrets for parties outside the territory of People's Republic of China includes:**

- Stealing, spying, buying, or illegally providing trade secrets for entities, organizations, or individuals outside the territory of China.

□ **Penalties:**

- 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."

Case

□ The Supreme People's Court recognizes punitive damages for malicious trade secret infringement, taking into account both actual damages and illicit gains

□ The Supreme People's Court recognizes the application of punitive damages for willful infringement of trade secrets, where the damages can be 1 to 5 times the actual loss or illegal gains

Business Support Program for MSMEs

□ In 2022, People's Republic of China's State Administration for Market Regulation (SAMR) announced an Central Innovative Pilot Program for Trade Secret Protection, encouraging all regions across People's Republic of China to plan and implement related initiatives.

□ The program focuses on strengthening innovation in trade secret protection systems, improving operational frameworks, enhancing supervision and enforcement mechanisms, and developing service and support systems while fostering an enabling environment. It requires each city- and region-level unit to propose specific tasks.

□ Accordingly, each city-level jurisdiction is implementing a 'Trade Secret Protection Innovation Pilot Project,' which includes specific measures to support enterprises participating in the project.

- (Shijiazhuang's Central Pilot Program Implementation Plan for Trade Secret Innovation (2025-2027)): Proposing specific measures to establish a regional trade secret protection system, identifying timelines for pilot programs, strengthening organizational leadership, increasing financial investment, and implementing support for social participation.
- For more information, please refer to: https://www.sjz.gov.cn/columns/22d15f71-611f-45a6-bb08-2c50cdb86a56/202505/30/385b3118-5ea3-4575-9453-c8e373633b51.html
- (Minhang District's Central Pilot Program Implementation Plan for Trade Secret Innovation (2025-2027): Regarding corporate support, proposes establishing a three-dimensional network for corporate support through measures such as building dispute resolution mechanisms, training specialized arbitration teams, and establishing regional trade secret protection guidance teams.
- For more information, please refer to: https://www.shanghai.gov.cn/gwk/search/content/deb01b7c2d6b494396d5bf6a66e9a7b5
- (Yinchuan City's Central Pilot Program Implementation Plan for Trade Secret Innovation (2025-2027)): Establishing trade secret protection bases and shelters, selecting and supporting pilot enterprises for trade secret protection and cultivation, building a social service network including setting up dedicated trade secret task forces within public organizations, conducting in-depth visits to enterprises, etc.
- For more information, please refer to: https://www.yinchuan.gov.cn/zzb/szfwj/202503/t20250303_4843656.html

□ As exemplified above, People's Republic of China is formulating specialized trade secret support strategies tailored to each region based on its strategy and implementing support for enterprises.

Hong Kong, China

Legal Framework

□ **Legal Basis:**

- No specific trade secret legislation
- Protection grounded in common law, most notably under the law of confidence

□ **Common Law Definition of Trade Secrets:**
Information—

- used in a trade or business
- confidential in nature, i.e. not already in the public domain
- easily isolated from other information which is free to use
- if disclosed to a competitor, liable to cause real or significant harm to the owner of the information
- the owner of the information 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

□ **Examples of Confidential Information that may be considered as Trade Secrets:**
Confidential information that is 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.

Civil Remedies

□ **Civil Claims Available:** Against unauthorized use or disclosure of confidential information

□ **Relief Options:** Injunctive reliefs (e.g. injunctions, delivery up of materials containing the confidential information in question) and monetary compensation (damages or account of profits)

□ **Injunctions granted when:** Monetary compensation is insufficient or risk of irreparable damage/harm exists

□ **Interim Injunctions:** May be granted by court to prevent the plaintiff from suffering irreparable damage/harm (e.g. risk of asset disposal or misuse of disputed information by the defendant) before substantive trial

Criminal Remedies

□ **Legal Basis:**

- No specific offence for misappropriation/misuse of trade secrets on its own
- An individual case involving misappropriation/misuse of trade secrets may be punishable by criminal law if and only if its overall circumstance and evidence 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 a specific criminal offence). In any event, criminal liability has to be determined on a case-specific basis.

Recommended Measure

□ Use of Non-Disclosure Agreements as far as practicable to specifically impose or reinforce the duty of confidence on the part of a party to whom the confidential information is to be imparted or who may be exposed to such information

Cases

□ *AXA China Region Insurance Company Limited v Pacific Century Insurance Company Limited and others [2003] 3 HKC 1* – Case law on what constitutes protectable trade secrets

□ *Conpak Management Consultants Limited v Luk Wai Ting [2024] HKDC 1545* — Case law denying infringement by not treating customer contact information as confidential

Business Support Program for MSMEs

□ Hong Kong, China provides intellectual property (IP) training programmes covering various IP-related topics (including trade secret protection) to local SMEs to assist them in building up their IP manpower capacity.

□ Moreover, Hong Kong, China provides various funding programmes and incubation programs for early-stage start-ups, and supports various initiatives relating to innovation, entrepreneurship, and the creation, protection and commercialisation of IP.

□ For more information, please refer to:

https://www.ip.gov.hk/en/key-programmes/ip-training-programme/index.html

https://www.itf.gov.hk/en/funding-programmes/index.html

https://www.hkstp.org/zh-cn/programmes/incubation/incubation-programme

Indonesia

Legal Framework

□ **Legal Basis:** Law No. 30 of 2000 concerning Trade Secrets (TSL)

□ **Definition of Trade Secrets (Article 1(1)):**

- Information not generally known to the public in the field of technology and/or business
- Has economic value due to its business usefulness
- Maintained as confidential by its owner

□ **Scope of Trade Secrets:**

- May include methods of production, processing, sales strategies, or other sensitive information related to technology or business operations
- Must be: not publicly known, economically valuable, and reasonably protected

□ **Requirements for Protection:**

- Information is known only to a limited group or not accessible to the public
- Information is used for commercial operations or economic advantage
- Owner takes adequate and appropriate measures to maintain confidentiality

□ **Rights of Trade Secret Owners:**

- Right to use, authorize others, or prohibit commercial use/disclosure

□ **Not Considered Misappropriation if:**

- Disclosure serves public security, health, or safety interests
- Reverse engineering is done independently for product development

Civil Remedies

□ **Enforcement Rights:**

- Owner or licensee may file claims for damages and injunctions
- Action may be taken against willful, unauthorized misappropriation
- Licensees have standing to sue under Indonesian law

Criminal Remedies

□ **Willful misappropriation punishable by:**

- Imprisonment up to 2 years, or fine up to IDR 300 million

□ Prosecution requires a formal complaint filed by the right holder, as the offense is complaint-based

Business Support Program for MSMEs

□ Indonesia does not appear to have a dedicated public support program specifically focused on trade secret protection.

□ However, in this regard, a Strategic Intellectual Property Assistance Program was held in 2024 to support small and medium-sized enterprises

□ The Strategic Intellectual Property Assistance Program was established to provide entrepreneurs with the knowledge and tools to navigate and utilize Indonesia's intellectual property system.

□ For more information, please refer to :

https://www.wipo.int/en/web/office-singapore/w/news/2024/kicking-off-the-strategic-ip-assist-program-in-indonesia

Japan

Legal Framework

□ **Legal Basis:**

- mainly by *the Unfair Competition Prevention Act (UCPA)*
- Supplemented by Civil Code provisions on torts, unjust enrichment, and contract law

□ **Definition of Trade Secret (UCPA Article 2(6)):** technical or business information useful for business activities, such as manufacturing or marketing methods, that is kept secret and not publicly known

□ **Acts constituting infringement under UCPA:**

- 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 (or while not knowing due to gross negligence) there has been a wrongful acquisition
- 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

Civil Remedies

□ **Subject to tort law limitation periods:**

- 3 years from knowledge of both damage and the identity of the perpetrator or 20 years from time of infringement, whichever is earlier

□ **Damage calculation methods (presumption provisions):**

- Lost profits (the amount of profit per unit of infringed things × quantity of the things transferred by the infringer)
- Infringer's profits (profit made by an infringer through the act of infringement)
- Equivalent to the royalties

Criminal Remedies

□ **Scope of Offense:**

- Acquiring trade secrets through theft, unauthorized access, or fraud, as well as unauthorized use or disclosure by subsiders
- If a person outside Japan uses the trade secrets of a trade secret holder conducting business within Japan, they may be subject to penalties

□ **Penalties:**

- Criminal sanctions, including for residents of another economies
- Proceeds derived from the offense may be Confiscated

Case

□ *Tokyo District Court, Judgment rendered on 19 February 2024, Case No.2022 (Wa) 70057 —* Information that constitutes a trade secret cannot be determined to be a trade secret infringement unless it is sufficiently 'specific' to be distinguished from general information

Business Support Program for MSMEs

□ Japan operates the Trade Secret Protection Support Services (INPIT) platform to assist companies in protecting trade secrets. INPIT's Trade Secret Consultation Desk provides services to SMEs and others, including support for extracting confidential information such as technical know-how, product ideas, and customer information; establishing management plans; and conducting seminars

□ It supports the management of confidential information and its protection as trade secrets. To this end, it dispatches intellectual property experts to companies to provide support. Companies can receive consultations on establishing management systems for trade secrets, countermeasures against trade secret leaks, strengthening information security measures, and intellectual property strategies for rights protection

□ The support provided by IP experts is limited to advising applicants on solving their specific challenges; they do not assume responsibility for the outcomes of the business activities. Therefore, they do not participate in contract negotiation meetings, perform specialized tasks such as drafting contracts or applications, or conduct IP searches, translations, or similar work.

□ For more information, please refer to:

https://www.inpit.go.jp/english/consul/TS_services.html

Republic of Korea

Legal Framework

□ **Legal Basis:**

- *Unfair Competition Prevention and Trade Secret Protection Act (UTA)*

□ **Definition of Trade Secret (under UTA):**

- Information not publicly known
- Has economic value
- Maintained through reasonable confidentiality efforts

□ **Scope:**

- Technical or managerial info (e.g., production methods, business strategies)

□ **Confidentiality Standard:** Active efforts required, though no fixed legal threshold

Civil Remedies

□ **Available Remedies:**

- Injunction to prohibit or prevent infringement
- Destruction of infringing goods and facilities
- Measures to prevent further misappropriation
- Remedies for reputational damage caused by intentional/negligent infringement

□ **Common Infringement Patterns:**

- Over 66.2% of cases involve former employees (2022 study)
- Misappropriation often occurs shortly before resignation
- Typical methods: starting a competing business or sharing secrets with new employer

Criminal Remedies

□ **Subject to Criminal Penalties:**

- Acquisition, use, or disclosure of a trade secret with intent to gain unjust benefits or cause damage
- Continued possession of trade secrets after a return or deletion request

□ **Aggravated penalties:** Where the trade secret is intended for use abroad

□ **Other punishable acts:**

- Damage, destruction, or alteration of trade secrets
- Attempts, preparatory acts, and aiding or abetting

Case

□ *Daejeon District Court, Decision 2022Gahap106228, 18 January 2024* — Case law that denied the economic usefulness of client information and did not recognize it as a trade secret

Business Support Program for MSMEs

□ 'Trade Secret Protection center' provides basic and advanced consulting services to help MSMEs establish effective trade secret management systems. It also offers legal advisory support in cases involving trade secret leakage and disputes

□ Trade secret protection training, trade secret protection consulting (basic/advanced), trade secret original proof services, distribution and operation of English secret management systems, legal advisory services for trade secret leakage disputes, and online/offline consultations provide comprehensive support throughout the entire lifecycle from trade secret creation to dispute response

□ Specifically, we provide foundational consulting on trade secret management systems for startups, SMEs, universities, and public institutions. Trade secret experts assess the company's current management status, identify issues, and propose achievable trade secret management plans tailored to the company's level

□ Based on comprehensive evaluation results, we present sector-specific vulnerabilities and an overall rating regarding the company's current trade secret management level. We identify problems and areas for improvement in each sector based on the trade secret management review results and propose improvement measures for the major trade secret management issues the company currently faces, recommending implementation actions that need to be carried out step by step

□ For more information, please refer to:

https://www.tradesecret.or.kr/main.do

Malaysia

Legal Framework and Recent Development

□ **Legal Basis:**

- No dedicated statute for trade secrets
- "Confidential information" referenced in the Trade Marks Act (TMA) and Trade Descriptions Act (TDA) for enforcement-related purposes

□ **Definition of Confidential Information (under TMA):**

- Trade, business, or industrial data belonging to any person
- Possesses economic value
- Not generally known or accessible to others
- Deemed confidential under the Act

□ **Acts Not Considered Infringement:**

- With owner's consent, anonymized, or already public
- Required for enforcement, statutory procedures, or investigations

□ **Legal Standard for Breach of Confidence (Coco v. A.N. Clark test, reaffirmed in CL Cosmetic Industries [2024]):**

- Information must be inherently confidential
- A duty of confidence must exist (express or implied)
- Unauthorized use or disclosure must cause harm to the owner

Civil Remedies

□ **Available Remedies:**

- Injunctions to prevent further misuse
- Monetary damages based on lost business profits

Criminal Remedies

□ **No specific law, but enforced via related statutes:**

- Trademarks Act: Penalizes unauthorized disclosure/use of confidential info obtained under statutory authority
- Penal Code: May apply where trade secrets are treated as "property"
- Computer Crimes Act: Criminalizes unauthorized access or transmission of access credentials
- Companies Act: Sanctions for misuse of confidential info or self-dealing by company officers

Case

□ *Dynacast (Melaka) Sdn Bhd v. Vision Cast Sdn Bhd* — This case holds that the protection period for confidential information can be set by contract for a specific period or permanently

Business Support Program for MSMEs

□ Malaysia does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for small and medium-sized enterprises

□ However, the SME implements all relevant ministries' and agencies' SME development programs. It operates a one-stop information portal for SMEs under its umbrella, providing advisory services covering all aspects of business operations for SMEs.

□ For more information, please refer to:

https://www.smeinfo.com.my/

Mexico

Legal Framework

□ **Legal Basis:**

- Federal Law on the Protection of Industrial Property (FLPIP)

□ **Definition of Trade Secrets (Art. 163, 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:**

- 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.

□ **Exceptions (Art. 164, FLPIP):**

- 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.

Civil Remedies

□ **Right to Claim:**

- Civil action available for misappropriation of trade secrets
- Claims allowed for foreign misappropriation if infringer is in Mexico, harm occurred in Mexico, or the secret relates to assets in Mexico

□ **Damages Assessment:**

- Market value of infringing goods or services
- Lost profits of the trade secret holder
- Gains obtained by the infringer
- Hypothetical license value based on comparable agreements

Criminal Remedies

□ **Definition of misappropriation:**

- Unauthorized use of trade secrets for competitive advantage or in breach of fair industrial/commercial practices
- Includes producing, offering, selling, importing, exporting, or storing products/services containing trade secrets without consent, where unfair competition is foreseeable

□ **Penalties:**

- Fines ranging from MXN 1,000 to MXN 300,000
- Imprisonment and fines for unauthorized acquisition, use, or disclosure that causes harm or creates unjust benefit

Case

□ Recognized only for matters subject to significant social condemnation in the context of punitive damages

Business Support Program for MSMEs

□ Mexico does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for small and medium-sized enterprises

□ Mexico estimates that micro and small enterprises constitute over 99.8% of all Mexican businesses and recognizes that SMEs play a decisive role in the Mexican economy. Accordingly, it aims to provide support through SME promotion policies to help them realize their potential and enter internal and global markets

□ To this end, it operates MIPYMESMX as a service platform for SMEs, providing guidance on key procedures required for SME operations. It also offers an SME self-assessment program, training, SME promotion policies, and customized workshops.

□ For more information, please refer to:

https://ventanillamipymes.economia.gob.mx/

New Zealand

Legal Framework

□ **Legal Basis:**

- Protected under common law (breach of confidence)
- Some criminal recognition under specific statutes

□ **Definition of Trade Secret:**

- Used or usable for industrial or commercial purposes
- Not generally known in relevant business circles
- Has actual or potential economic value
- Subject to reasonable secrecy measures

Civil Remedies

□ **Legal Basis:**

- No specific statute for civil enforcement
- Protection based on breach of confidence under common law

□ **Key Features:**

- No need for a formal contract—duty may arise from circumstances
- Doctrine grounded in equitable principles and good faith
- Recognized by Court of Appeal as a flexible, general protection

Criminal Remedies

□ **Legal Basis:**

- Section 230(1) of the Crimes Act 1961

□ **Offense Elements:**

- Dishonestly taking or copying items containing trade secrets
- Without proper authority and with intent to cause loss or gain benefit
- Knowing that the material embodies a trade secret

□ **Penalty:**

- Up to 5 years' imprisonment

Case

□ In the case of New Zealand courts, originality, economical value, and the effort required to create the information are considered when determining whether information is confidential

Business Support Program for MSMEs

□ New Zealand does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for SMEs, as the protection of trade secrets is primarily governed through general legal principles rather than a standalone statutory framework

□ However, services are provided to support small and medium-sized enterprises (SMEs). Business.govt.nz offers guidance tailored to the specific needs of SMEs across their entire lifecycle—from start-up and growth to ongoing management.

□ For more information, please refer to:

https://www.business.govt.nz/

□ Additionally, by leveraging opportunities such as education, networking, and on-site consulting through the regional business network, participants can utilize the regional expert and resource network.

□ For more information, please refer to:

https://www.business.govt.nz/strategy-and-performance/regional-business-partner-network

Papua New Guinea

Legal Framework

□ **Legal Basis:**

- Based on English common law system
- Statutes and underlying law (common law, equity, customs)

□ **No Dedicated Statute for Trade Secrets:**

- Trade secrets protected under common law principles
- Adjudicated case-by-case by courts

□ **Definition and Scope of Trade Secrets:**

- Inventions, techniques, or confidential business information kept undisclosed for competitive advantage
- May also include traditional knowledge (e.g., medicinal plant use, extraction techniques, ecological information)

□ **Protection of Indigenous Knowledge:**

- Protected as trade secrets where confidentiality agreements exist
- Recognized particularly when tied to commercial partnerships with third parties

Civil Remedies

□ **Legal Basis:**

- Equitable doctrine of breach of confidence (derived from English common law)
- Contractual obligations under employment agreements

Criminal Remedies

□ **Legal Basis:**

- No dedicated criminal statute specifically for trade secrets
- Misappropriation may be prosecuted under related laws

□ **Applicable Laws and Offenses; Protection of Private Communication Act 1973:**

- Penalizes unauthorized interception or disclosure of private communications via surveillance devices
- Includes punishment for disclosing or disseminating intercepted content

□ **Criminal Code Act:**

- Penalizes public service employees who improperly publish or deliver secret documents or information
- Punishable by up to two years' imprisonment

Business Support Program for MSMEs

□ Papua New Guinea does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for SMEs

Peru

Legal Framework

□ **Legal Basis:** Decision 486 of the Andean Community; and Peru's Legislative Decrees No.1075 and No.1044

□ **Legal Criteria:**

- 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.

□ **Scope of Protection:**

- Covers product features, manufacturing methods, marketing strategies, etc.
- Recognized as part of industrial property under Decree No.1075

□ **Prohibited Conduct:**

- Unauthorized use or disclosure in breach of contractual or employment duties
- Illicit acquisition or third-party misuse
- Acts causing unfair advantage or harm

□ **Examples of Unfair Practices:** Espionage, breach of duty, or inducement

Civil Remedies

□ **Interim measures (Art. 33.2, Decree No.1044):**

- 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

□ **Corrective Measures (Art. 55.1, Decree No.1044):**

- The cessation of the act of 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, of 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

Criminal Remedies

□ **Lack of Specific Criminal Provision:**

- No dedicated criminal law addressing trade secret misappropriation
- Article 222: regulates industrial property, excludes trade secrets
- Article 165: penalizes unauthorized disclosure of confidential info by professionals, not tailored to trade secrets
- No comprehensive criminal framework for trade secrets in commercial settings

Case

□ INDECOPI determined that commercial espionage constitutes trade secret infringement and considered that securing objective evidence is crucial for proving trade secret infringement

Business Support Program for MSMEs

□ Peru does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for SMEs

□ While Peru operates a range of support programs and financing mechanisms for MSMEs, it is not clearly evident from available information that these initiatives are specifically aimed at enhancing trade secret protection

The Republic of the Philippines

Legal Framework and Recent Development

□ **Legal Basis:**

- No standalone statue for trade secrets in the Republic of the Philippines
- Confidential business information recognized under IP and competition laws

□ **Definition of Trade Secret:**

- Covers operational, production, sales, shipment, purchase, and financial data
- Includes plans, processes, tools, mechanisms, and non-patented formulas providing economical advantage
- Recognized in *Air Philippines Corp. v. Pennswell, Inc.* (G.R. No. 172835, Dec. 13, 2007)

□ **Scope of Protection:**

- Encompasses operational procedures, pricing models, catalogues, and customer lists
- Information must not be public and must confer competitive advantage

□ **Criteria:**

- Non-publicity and Economical value
- Limited disclosure within a trusted relationship

Civil Remedies

□ **Enforcement Mechanisms:**

- Use of confidentiality clauses in employment and service contracts
- Breach of such clauses may result in civil liability for damages

□ **Third-Party Liability (Civil Code, Art. 1314):**

- Liability for knowingly inducing breach of valid contract
- Must prove contract existence, third party's knowledge, and lack of legal justification

Criminal Remedies

□ **Legal Basis:**

- The Competition Act – prohibits unauthorized disclosure of confidential business information submitted to the authority.
- Revised Penal Code (Art. 292) – penalizes employees who disclose industrial secrets causing harm to the owner

□ **Applicable Sanctions:**

- Revised Penal Code (Art. 292) – penalizes employees who disclose industrial secrets causing harm to the owner
- Imprisonment or fines under the Penal Code

Case

□ *Cocoland Development Corporation v. Public Labor Relations Commission* — Case where objective and substantive grounds were deemed necessary for determining confidentiality

Business Support Program for MSMEs

□ The Republic of the Philippines does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for SMEs

□ However, the Republic of the Philippines offers various support programs for MSMEs—such as financing-schemes and business development services—though it is not evident from available information that any of these initiatives are specifically aimed at trade secret protection

The Russian Federation

Legal Framework

□ **Legal Basis:**

- Civil Code of the Russian Federation (Part IV, Chapter 75)
- Federal Law No. 98-FZ on Trade Secrets (2004)
- Federal Law No. 135-FZ on the Protection of Competition (2006)
- Criminal Code of the Russian Federation

□ **Definition of Trade Secret (Civil Code Art. 1465(1)):**

- Information of any nature (e.g., production, technological, economic) related to intellectual activities or professional methods
- Must have economical value due to secrecy
- Not publicly known or legally accessible to third parties
- Subject to confidentiality measures through a trade secret regime

□ **Exclusions from Protection (Art. 1465(2)):**

- Information required to be disclosed by law
- Information not subject to lawful restriction

□ **Minimum Protective Measures (Trade Secret Law Art. 10(1)):**

- Designation of information classified as trade secrets
- Controlled access procedures and compliance monitoring
- Recordkeeping of individuals with access
- Contractual regulation of use in employment or civil agreements
- Labelling materials with “Trade Secret” stamp and holder’s identity

□ **Exclusive Rights (Civil Code Art. 1466):**

- Right to use trade secret information by lawful means, including manufacturing or organizational use
- Right to assign or license the trade secret
- Independent right arises for individuals who access the secret in good faith and without violating others’ rights

Civil Remedies

□ **Trade Secret Law Article 14(1):**

- Applicable liability: disciplinary, civil, administrative, or criminal
- Triggered by violation of trade secret obligations

□ **Civil Code Article 1472:**

- Right to file civil claim for unauthorized use or disclosure
- Protection scope: exclusive rights to know-how (production secrets)
- Available remedies: compensation for economic loss

□ **Trade Secret Law Article 6.1(6):**

- Legal protection against third-party infringement
- Infringing acts: illegal acquisition, unauthorized disclosure, improper use
- Available relief: cessation of use and monetary compensation

□ **Requirements for Civil Action:**

- Proof of lawful ownership or control of trade secret
- Evidence that information met confidentiality criteria
- Proof of unauthorized use, disclosure, or exploitation
- Violation must exceed scope of permitted contractual use

□ **Legal Limitations:**

- Filing deadline: within 3 years of discovering violation and infringer
- Limitation applies regardless of actual damages incurred
- Failure to meet deadline may forfeit right to legal remedy

Criminal Remedies

□ **Criminal Offenses (Article 183, Criminal Code):**

- unlawful acquisition - Bribery of insiders or employees / Theft of documents or data storage devices / Intimidation, coercion, or blackmail / Imprisonment, depending on severity
- Unauthorized disclosure or use of commercial secret information - Revealing trade secret information without the owner's consent / Utilizing such information in a way that violates legal or contractual duties / Gaining personal or economical advantage from misappropriated secrets

□ **Criminal Sanctions:**

- Monetary fines imposed by judicial authorities
- Corrective labor as an alternative to incarceration
- Imprisonment, depending on severity

□ **Degree of Punishment:**

- The method used in the criminal act (e.g., coercion vs. theft)
- The scope and scale of harm caused to the trade secret holder
- Whether the act was committed with intent or as part of an organized effort

Case

□ According to an analysis report on judicial practices in the Russian Federation, even if an employee discloses information learned in the course of their duties to an external party, dismissing that employee solely on the grounds of disclosure is deemed unlawful if the employer cannot prove that the disclosed information contained trade secrets

Business Support Program for MSMEs

□ The Russian Federation does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for SMEs

□ While the Russian Federation operates a range of support programs and financing mechanisms for SMEs, it is not evident from available information that any of these initiatives are specifically aimed at enhancing trade secret protection

□ However, in the Russian Federation, it is understood that numerous private companies exist whose business is the management and protection of trade secrets

□ For example, the Data Security Center (Центр безопасности данных) provides comprehensive services for protecting confidential information (trade secrets, proprietary information, and personal data) and critical information infrastructure. The Data Security Center is a specialized agency licensed by the Federal Service for Technical and Export Control (FSTEC) of the Russian Federation for the technical protection of confidential information.

□ For more information, please refer to:

https://data-sec.ru/

□ SEARCHINFORM provides training for trade secret protection and recommends utilizing DLT systems as a technical means for protection.

□ For more information, please refer to:

https://searchinform.ru/resheniya/biznes-zadachi/zaschita-kommercheskoj-tajny/

Singapore

Legal Framework

□ **Legal Basis:**

- No dedicated statute for trade secrets
- Civil protection through common law (e.g. contract law, law of confidence)

□ **Test for Breach of Confidence:**

- information must possess the quality of confidentiality
- information must be shared under an obligation of confidence
- claimant shows information has been misused or disclosed without authorization, or defendant to prove that their acquisition of the information was not unconscionable

□ **Public Interest Exception:**

- Disclosure may be justified if clearly serving public interest

Civil Remedies

Available Remedies:

- Injunctions to stop misuse
- Monetary compensation (damages or profit account)
- Order to destroy or return confidential materials

□ **Procedural Considerations:**

- Possible defenses: inadvertent use, lack of knowledge, public interest
- Limitation period: 6 years from breach or 3 years from knowledge of breach, whichever is later

Criminal Remedies

□ **Legal Basis:**

- Computer Misuse Act 1993 applies; no direct criminalization of trade secret theft

□ **Offenses:**

- Unauthorized access, copying, or extraction of data
- Access with intent to cause loss, commit fraud, or gain advantage
- Unauthorized sharing or transfer of access credentials

□ **Penalties:**

- Fine and/or imprisonment, with harsher penalties for intent-based offenses

Case

□ When considering whether a trade secret exists the court considers the nature of employment, the character of the information, confidentiality notice, and distinguishability from public information when determining whether a trade secret exists in an employment context

Business Support Program for MSMEs

□ Singapore does not appear to have a dedicated public support program specifically focused on trade secret protection for SMEs

□ However, Singapore offers a broad range of support programs and funding schemes designed for SMEs—including grants for capability development, digital transformation and business growth.

□ The Intellectual Property Office of Singapore (IPOS) has published a trade secrets guide to help businesses and other entities more effectively protect and manage their trade secrets. This guide includes examples of tools and services that businesses can utilize, such as a framework for enterprises to protect and manage their trade secrets, and factors to consider when drafting non-disclosure agreements and confidentiality clauses.

IPOS also supports SMEs by facilitating IP Business Clinics, which provide advice on IP protection and management, and IP Legal Clinics, which offer preliminary advice to enterprises facing IP disputes. Both services may extend to trade secret matters.

□ For more information, please refer to:

https://www.ipos.gov.sg/about-ip/trade-secret/#32ffb0554455bbb846b40835775f182e

https://www.ipos.gov.sg/eservices/ip-clinics/

https://ipgrow.gobusiness.gov.sg/knowledge-hub/ip-business-clinic

Chinese Taipei

Legal Framework

□ **Legal Basis:** Trade Secrets Act (TSA) - governs trade secrets in Chinese Taipei

□ **Definition (Art. 2):**

- Non-public information with economic value
- Subject to reasonable secrecy measures
- Applicable to production, sales, or business activities

□ **Misappropriation (Art. 10):**

- Acquisition through improper means
- Unauthorized use or disclosure with intent, gross negligence, or statutory duty breach

□ **Improper Means:**

- Theft, fraud, coercion, bribery, unauthorized duplication
- Breach or inducement of breach of confidentiality obligations

Civil Remedies

□ **Liability:**

- Intentional or negligent infringement incurs damages liability
- Joint infringement entails joint and several liability

□ **Time Limits:**

- File within 2 years of discovery and no later than 10 years from the date of the infringing act

□ **Damages:**

- If unprovable, presumed as lost profit different
- Willful cases: punitive damages up to 3x unlawful gain

Criminal Remedies

□ **Liability:**

- Misappropriation for unlawful benefit or to harm the holder punishable by fines or imprisonment
- Attempted misappropriation also punishable

□ **Enhanced Penalties:**

- If benefit exceeds statutory fine – up to 3x unlawful gain
- For the purpose of overseas use – up to 10 years' imprisonment
- For the purpose of overseas use with benefit exceeding standard fine – 2-10x unlawful gain

□ **Procedural Aspect:** Prosecution requires a formal complaint by rights holder

Case

□ Regarding the assessment of confidentiality management, if a company has implemented tiered control measures based on whether there is a necessity for employees to access or use trade secret information, whereby employees without such necessity cannot readily become aware of its contents, the company may be deemed to have adopted reasonable confidentiality measures.

Business Support Program for MSMEs

□ Taiwan Association for Trade Secrets Protection (TTSP)

- TTSP, as a non-profit organization, does not provide public support for trade secret protection. However, it serves as a platform for sharing information on trade secret protection enhancement, legal amendment advice, and related issues with the central authorities and industry. It also promotes global awareness and cooperation regarding trade secret protection in Chinese Taipei.
- For more information, please refer to:

  https://www.ttsp.org.tw/

□ Taiwan Intellectual Property Office (TIPO)

- TIPO has established a dedicated webpage for trade secret protection, providing frequently asked questions, basic guides, relevant regulations and key rulings, checklists for small and medium-sized enterprises, and practical training manuals.
- For more information, please refer to:

  https://www.tipo.gov.tw/tw/tradesecrets

Thailand

Legal Framework and Recent Development

□ **Definition:**

- Protected under Trade Secret Act (No.2) B.E. 2558 (2015)
- Business information with economical value from secrecy and reasonable confidentiality measures
- Includes formulas, patterns, programs, methods, techniques, processes, or other meaningful data

□ **Rights of Owner:** Disclose, withhold, use, or authorize use

□ **Misappropriation:**

- Unauthorized disclosure, taking, or use contrary to honest commercial practices
- Examples – breach of contract/confidence, bribery, coercion, fraud, theft, unauthorized electronic acquisition

□ **Exceptions:**

- No knowledge of improper means, public health or safety disclosure by authorities, independent discovery or development, lawful reverse engineering, etc.

Civil Remedies

□ **Injunctions:**

- Preliminary injunction to stop misappropriation
- Permanent injunction possible with damages claim

□ **Limitation Period:** 3 years from discovery or 10 years from act, whichever is earlier

□ **Damages:**

- Presumed misappropriation if identical product and no counter-evidence
- Compensation for losses and profits; punitive damages up to twice compensatory

Criminal Remedies

□ **Penalties:**

- Obstructing or failing to cooperate with officials - up to 1 year or 1 month imprisonment, fines up to THB 20,000 or THB 2,000
- Using or disclosing to harm business - up to 2 years imprisonment, fine up to THB 200,000
- Disclosing secrets from official duties - up to 1 year imprisonment, fine up to THB 100,000

Case

□ *Thailand Supreme Court Decision No. 10217/2553* — A case holding that a general non-disclosure and non-compete clause in an employment contract alone is insufficient to establish trade secret protection, requiring specific identification of the subject matter and proof of substantive protection

Business Support Program for MSMEs

□ Thailand does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for SMEs

□ Thailand operates a variety of support programs and financing mechanisms for SMEs though it is not evident from available information that any of these initiatives target trade secret protection specifically

United States

Legal Framework

□ **Legal Basis:**

- Federal - DTSA, CFAA, EEA / State - mostly UTSA; NY excluded, but DTSA applies

□ **Definition of EEA and DTSA:**

- Covers all forms/types of financial, business, scientific, technical, economic, or engineering information (tangible/intangible)
- Conditions - (1) reasonable measures to keep secret, (2) independent economic value from secrecy

□ **Definition of UTSA:**

- Information includes formula, pattern, compilation, program, device, method, technique, process, etc.
- Conditions: (1) independent economic value from secrecy, (2) reasonable efforts to maintain secrecy

□ **Misappropriation:**

- Acquisition by improper means
- Unauthorized disclosure/use by person who (1) acquired by improper means, or (2) knew/had reason to know that trade secret was (a) derived from person who acquired by improper means, (b) acquired with duty to maintain secrecy/limit use, (c) acquired by accident or mistake, or (d) derived from person with duty to maintain secrecy/limit use

□ **Improper Means:**

- Theft, bribery, misrepresentation, breach of duty, espionage; reverse engineering, independent derivation, & other lawful means of acquisition are excluded

□ **Inevitable Disclosure Doctrine (IDD):**

- In some states, courts will enjoin former employees, for a limited time, from beginning employment in roles likely to lead to trade secret use, without a showing of actual proof
- Injunctive relief factors include: degree of competition, job similarity, trade secret value, actual misappropriation

Civil Remedies

□ **Injunctive Relief:**

- Granted to prevent actual or threatened misappropriation
- Cannot prevent entering employment, but can place conditions on employment based on evidence of threatened misappropriation

□ **Ex Parte Civil Seizure (18 U.S.C. §1836(b)(2)(A)(i)):**

- Granted without prior notice in extraordinary circumstances
- Requires proof of immediate & irreparable harm, balance of harms favoring applicant, plus other statutory requirements

□ **Exclusion Order/Seizure and Forfeiture Order (19 U.S.C. § 1337):**

- Granted upon a determination made by United States International Trade Commission that the importation of an article misappropriates a trade secret and constitutes an unfair method of competition
- The Order directs Customs to stop infringing imports from entering United States
- In addition, the ITC may issue cease and desist orders against named importers and other persons engaged in trade secret misappropriation

□ **Monetary Damages:**

- Recovery for actual loss plus any unjust enrichment not included in actual damages, or a reasonable royalty
- Limited to the period the info is a trade secret + any period of retained competitive advantage

□ **Exemplary Damages:**

- Up to 2x actual damages for willful and malicious misappropriation

Criminal Remedies

□ **18 U.S.C. §1831 – Economic Espionage:**

- Misappropriation intended or known to benefit a foreign government, instrumentality, or agent
- Covers theft, copying, transmission, alteration, destruction, delivery (physical/electronic), attempts/conspiracies, etc.
- Penalties for individuals – up to 15 years' imprisonment and fines up to USD 5 million
- Penalties to organizations – up to USD 10 million or 3x value of stolen trade secret (whichever is greater)

□ **18 U.S.C. §1832 – Theft of Trade Secrets:**

- Misappropriation of a trade secret related to product/service used in interstate or foreign commerce, for the benefit of anyone other than the owner and intending/knowing that the owner will be injured
- Covers theft, copying, transmission, alteration, destruction, delivery (physical/electronic), attempts/conspiracies, etc.
- Penalties to individuals – up to 10 years' imprisonment and fines
- Penalties to organizations – up to USD 5 million or 3x value of stolen trade secret (whichever is greater)

□ **Key Distinction:**

- §1831 - targets conduct benefiting foreign interests
- §1832 - targets theft for commercial or economic gain by anyone other than the trade secret owner (lesser penalties than §1831)

Business Support Program for MSMEs

□ The USPTO provides resources for policy leadership and technical expertise in trade secret protection, including the Trade Secrets and Intellectual Property Toolkit and online video materials.

□ For more information, please refer to: https://www.uspto.gov/ip-policy/trade-secret-policy

Viet Nam

Legal Framework

□ **Legal Basis:**

- Governed by the Law on Intellectual Property
- Trade secret: information from financial or intellectual investment, undisclosed, and usable in business
- Rights established by lawful acquisition and maintaining confidentiality

□ **Protection Criteria:**

- Not common knowledge or readily accessible, provides competitive advantage in business use, necessary measures taken to maintain secrecy

□ **The Use of a Trade Secret:**

- Applying in manufacturing, services, or commercial transactions
- Importing, advertising, or storing goods produced using the trade secret

□ **Exclusions from Protection:**

- Personal secrets, public administrative secrets
- Public defense or security secrets
- Non-business-related information

□ **Ownership:**

- Owner - lawfully acquires and maintains secrecy
- Secrets created in assigned tasks belong to employer unless otherwise agreed

□ **Infringements:**

- Acquiring by breaching confidentiality measures
- Disclosing/using without owner's consent
- Violating agreements; obtaining via deception, bribery, coercion, or abuse of trust
- Obtaining from agencies by bypassing confidentiality measures
- Using/disclosing knowing it was unlawfully acquired
- Failing to fulfil legal confidentiality obligations

Civil Remedies

□ **Rights of IP Holders:**

- Adopt technical measures to prevent infringement
- Request infringer to cease acts, provide a public apology, and pay damages
- Request competent authorities to take enforcement action
- File lawsuits to protect legal rights and interests

□ **Types of Civil Remedies:**

- Injunctions (cessation of infringement)
- Mandatory public apology
- Enforcement of civil obligations
- Compensation for damages (material and non-material)

□ **Compensation Principles:**

- Damages calculated based on actual loss suffered
- May cover economic and emotional/reputational harm
- Court determined amount if actual harm is proven

Criminal Remedies

□ **Article 159:**

- Prohibits unauthorized access, collection, or disclosure of confidential communications or information
- Covers acts such as illicit acquisition, destruction, concealment of documents, illegal eavesdropping, or unauthorized searches/seizures
- Penalties - fines, community service, or imprisonment in serious cases

□ **Article 288:**

- Criminalize Illegal provision or use of personal or confidential data via computer or telecommunications networks
- Includes unauthorized publication, sale, or disclosure of such data
- Applicable to digital misappropriation of trade secrets
- Covers digital misappropriation of trade secrets; aggravated penalties for large-scale or high-impact acts

□ **Article 289:**

- Prohibits unauthorized access to computer networks or devices, including hacking, privilege abuse, or data theft
- Includes manipulation, exploitation, or destruction of data
- Severe penalties for breaches affecting public security or critical infrastructure

Case

□ *Case No. 09/2010/LD-ST (10 December 2010)* — Regarding trade secret infringement cases, if internal company regulations are lawfully established and disclosed, disciplinary actions or dismissals based on such regulations are deemed valid

Business Support Program for MSMEs

□ Viet Nam does not appear to have a dedicated public support program specifically focused on trade secret protection or on trade secret protection for SMEs

□ However, through irregular intellectual property management training and consulting programs, we provide intellectual property consulting support for companies within these programs

□ For example, the Intellectual Property Management Clinic (IPMC) education and consulting program was held in October 2025. This program aims to promote innovation by supporting companies in establishing comprehensive intellectual property strategies to protect and enhance the value of their intellectual property rights. IPMC 2025 selected 15 companies to provide one-on-one consulting on business models analyzed from an intellectual property perspective and proposed ways to build effective intellectual property strategies tailored to each business environment.

□ For more information, please refer to:

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