




# TRADE SECRETS ENTERPRISE GUIDE

GUIDING ENTERPRISES IN THE  
PROTECTION AND MANAGEMENT OF  
TRADE SECRETS IN SINGAPORE

Copyright © 2022 Intellectual Property Office of Singapore

You may download, view, print and reproduce this document  
without modifications, but only for non-commercial use. All  
other rights are reserved.



This Guide is meant to serve as an introductory and practical reference for enterprises who are looking to learn about, identify, protect and manage their trade secrets. This Guide is for information and reference, and is not intended to be exhaustive.

This document is made available on an “as is” basis and all implied warranties are disclaimed. It does not constitute, and should not be relied upon, as legal advice. For in-depth information specific to your business needs, always consult a legal professional. No recommendation, suggestion as to suitability or quality, or referral of any service providers are made, or intended, in this Guide.

# FOREWORD

---

The Singapore IP Strategy 2030 (“SIPS 2030”) released in April 2021 is our national roadmap for maintaining a world-class Intangible Asset (“IA”) / Intellectual Property (“IP”) regime to support innovative businesses in using their IA/IP for growth.

As part of SIPS 2030, the Intellectual Property Office of Singapore (“IPOS”) undertook a study in 2021 to gain a deeper understanding of Singapore’s trade secret regime vis-à-vis other comparable economies. The study also sought to find out the level of knowledge and ability of enterprises operating in Singapore to protect and manage their trade secrets; and how they might be supported, especially in this era of rapid technological advances.

The study found that most enterprises recognised the importance of trade secrets for their business growth, with about 75% of enterprises considering trade secrets to be the most important to their business. That said, about half of all enterprises were not familiar with Singapore’s trade secret regime, and about 2 in 5 enterprises did not use any trade secret-related services. Most enterprises indicated that more can be done to support enterprises in the protection and management of their trade secrets. These includes raising awareness of the importance of trade secrets and increasing the accessibility of trade secret-related services.

Similar findings were also observed at the inaugural trade secrets event held in July 2022 and co-organised with the Singapore Business Federation (SBF). Entitled “Keep your Secrets, Protect your Trade: How to Effectively Protect and Manage Trade Secrets for Business Growth” this event saw more than 130 participants from diverse industries in attendance. While most participants indicated that their company had trade secrets, less than one-third believed that their trade secrets were adequately protected and managed.

In response to the enterprises’ needs, IPOS has commissioned Bird & Bird ATMD LLP to develop this Trade Secrets Enterprise Guide which includes non-exhaustive examples of available trade secret tools and services that enterprises may tap on. We would also like to thank our industry partners, including Action Community for Entrepreneurship, Enterprise Singapore, SGTech, SBF, and Singapore FinTech Association, for their support on the Guide. Apart from this Guide, IPOS will continue working with our industry partners on other resources and in other ways to raise awareness and build enterprise capabilities in protecting and managing trade secrets.

For further enquiries about IP, you may reach out to IPOS - visit [www.ipos.gov.sg](http://www.ipos.gov.sg) or contact us or call 63398616.

For information about trade secrets, including this study report, please visit our IPOS’ website at - <https://www.ipos.gov.sg/about-ip/trade-secrets>.

# 1. INTRODUCTION

---

## What are trade secrets?

As businesses expand and continue to innovate, they develop valuable know-how and information to help them remain competitive. Often, a company's success is tied to how effectively it can exploit such commercial information and prevent it from falling into the hands of its competitors.

Broadly speaking, such know-how and commercial information are a company's "**trade secrets**". Trade secrets generally have the following qualities:

### Qualities of Trade Secrets

- They are "**secret**" i.e., not known by the public and not readily accessible by employees of the company;
- The information is **valuable** because it is secret; and
- The business has taken **reasonable steps to protect** the secrecy of the information. This will involve restricting the access of the information to only a few employees, emphasising the secrecy of the information, and isolating this information from other information which employees are free to access, use or disclose.

Once the information has these qualities, it is automatically protected as a trade secret and there is no need to 'register' the information as a trade secret.

As long as the information remains secret and is not independently discovered or reverse engineered by others, it can remain a trade secret indefinitely (i.e., there is no expiry or end date to a trade secret).

- Examples of trade secrets include secret manufacturing processes, recipes, technical systems, commercially sensitive information, management procedures and trading practices, company accounts books and customer lists.
- **Famous examples of trade secrets:** Google's search engine algorithm; the ingredients of Kentucky Fried Chicken's chicken recipe; the formulas behind WD-40 and Listerine; the methodology of the New York Times Best-Seller List.

## Trade secrets – Intellectual Property

Trade secrets are protected as a form of intellectual property ("**IP**") which broadly refers to creations of the mind, e.g., inventions, literary and artistic works, brand names and logos.

A company typically has multiple different forms of IP that can be protected and commercialised, e.g., trade marks, patents, copyright.

Trade secrets can complement other forms of IP protection. For example:

- Innovative ideas and solutions can be protected as trade secrets before they are eventually protected and disclosed through Patents.
- Spreadsheets containing customer data can also be protected under Copyright law.
- Your mobile applications may feature your brand (protected under Trade Mark law) and the graphical user interface (protected as a Registered Design or under Copyright law). The software for the application could be patentable, and any customer data collected through the application can also potentially be protected as a Trade Secret.

In the following Sections, the Guide will set out an overview of how your trade secrets can be (i) protected, (ii) managed, and (iii) commercialised in order for your business to grow effectively.

## 2. LEGAL FRAMEWORK FOR TRADE SECRET PROTECTION IN SINGAPORE

In this Section, the Guide aims to cover the legal framework for trade secret protection in Singapore.

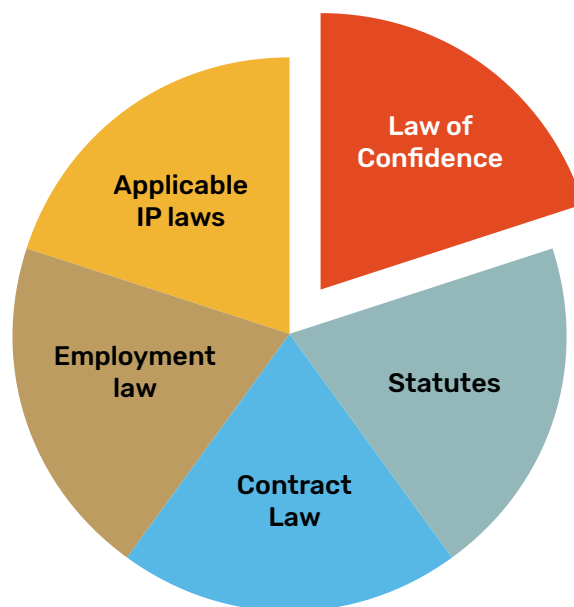
### Overview

In Singapore, your trade secrets are protected primarily through the **law of confidence**.

- The law of confidence protects all types of confidential information, such as your personal/private information (e.g., medical reports, photographs, receipts).
- However, being highly secret and valuable commercial information, trade secrets receive enhanced protection under the law of confidence.

#### Did you know?

The information that can be protected under the law of confidence can be simple in nature e.g., drawings, spreadsheets. It also does not have to be written down e.g., oral recipes.



### Laws which can protect your trade secrets

Depending on the facts of the case, your trade secrets can also be protected by other areas of IP, Employment and Contract Law, although these areas will not be explored in detail in the Guide.

The Computer Misuse Act 1993 ("**CMA**") may also apply in cases where your cybersecurity has been breached by a person seeking to obtain your trade secrets. Under the CMA, it is an offence for persons to knowingly cause a computer to perform a function in order to gain unauthorized access to any programme or data held in any computer (section 3(1) of the CMA).

This provision covers scenarios, for example, where ex-employees access a company's servers to obtain files/information for their own benefit. Offenders can be fined and/or imprisoned, and be made to compensate the business if damage is done to the business' computer, programme or data.

## Introduction to the law of confidence

The law of confidence protects your confidential information (including your trade secrets) against unwanted disclosure and/or acquisition by third parties.

To qualify for protection, it must be shown that:

### Criteria to qualify

- (a) The information sought to be protected was confidential in nature;
- (b) The information was imparted in circumstances where an obligation of confidentiality was imposed; and
- (c) There was a breach of this obligation of confidentiality.

[Each of (a) to (c) will be covered in 2.1 to 2.3 respectively below.]

### 2.1 Whether the information is confidential

First, to qualify for protection, your information must be considered 'confidential' in nature.

The simplest example of this is where information is kept only within a company.

However, even in situations where persons outside your company know about the information / trade secret, the information can still be considered confidential if it has not become generally known or readily accessible to the public.

Ultimately, it will need to be considered whether the degree or extent of disclosure (if any) would be such that it would be fair to treat the information as 'confidential'. The factors that will be taken into account are as follows:

#### What type of information is this?

- Is it already known or easily accessible to the public?

**Example:** The concept of the "ticketless" carpark system is not in itself 'confidential' because it can be easily observed by anyone visiting the carpark.

On the other hand, commercially sensitive information known only to a few senior employees is likely to be considered confidential.



#### If the information was disclosed to third parties:

- How/why was it disclosed?
- How widespread was the disclosure?
- Was there a non-disclosure agreement in place?

**Example:** A company's drawings were found to be confidential even when they were published in its operating manuals, because it was for the limited and specific purpose of its customers' use. There was also no evidence that these drawings were widely disseminated.



#### If the information can be found online:

- Was it actually accessed by the public?
- Can it only be understood by people with expertise/skill?

**Example:** Although emails from a company's computer system were uploaded online to Wikileaks, they were still considered confidential because they only formed a small part of all the data that was uploaded and it was unlikely that the public would in fact have accessed these emails.



#### Steps taken to protect information:

- Was it clear that the document/information was confidential?
- Were steps taken to make information inaccessible?

**Example:** Password protection; marking documents as 'Confidential'; only allowing a certain seniority of employees to access document/information.

## 2.2 Whether an obligation of confidence exists

Second, to qualify for protection, it must also be shown that the recipient of the information was under an obligation (i.e., duty) of confidence to protect the confidentiality of the information.

This obligation of confidence may arise in a few ways:

Contract	Equity
<ul style="list-style-type: none"><li>■ Involves a contract with express (i.e. explicit) or implied terms prohibiting the recipient from using or disclosing the confidential information.</li><li>■ In such cases, a claim for breach of contract may also arise.</li><li>■ <b>Examples:</b><ul style="list-style-type: none"><li>• Employment contract</li><li>• Non-disclosure agreement</li></ul></li></ul>	<ul style="list-style-type: none"><li>■ When a person is found to have received information that he knows or ought to know to be reasonably regarded as confidential, an obligation of confidence may be found.</li><li>■ <b>Examples:</b><ul style="list-style-type: none"><li>• Accessing information that is password protected or documents marked 'confidential'/'patent pending'/'legal privilege'</li><li>• Taking confidential documents via illegal means</li></ul></li></ul>

Most scenarios involving a breach of confidence or the misappropriation of trade secrets occur in the employment context. This typically involves employees or ex-employees using or disclosing their (former) employer's confidential information and/or trade secrets.

Even where there are no explicit confidentiality clauses in the employment contract, the Singapore courts have decided that an employee will still be bound by the following obligations:

- While employed, the employee may not use or disclose a company's confidential information except in the discharge of his/her duties as an employee. This means, for example, that the employee cannot use the company's confidential information to moonlight for a competitor.
- After his/her employment, the employee should not use/disclose your trade secrets, as they are **highly secret** in nature.
- The courts will consider the following factors holistically in assessing whether the confidential information is so confidential as to enjoy protection as a 'trade secret':
  - **The nature of the employment:** If the employee routinely handles confidential information, he/she is much more likely to be considered to have been handling trade secrets as opposed to employees with minimal or no exposure to confidential information.
  - **The nature of the information:** If the information was circulated widely and easily accessible within the organisation, it is less likely to be considered a 'trade secret' as compared to information accessible to only a select few employees.
  - **Whether the confidentiality of the information was impressed on employees:** This may involve marking confidential documents as "CONFIDENTIAL", putting measures in place to secure these documents and educating your employees on the confidentiality of the information. See further **Sections 3.3** and **3.4** below.
  - **Whether the information can be easily isolated or separated from other information which employees are free to use or disclose:** If the information cannot be isolated or separated from other non-confidential information, it is unlikely to be considered a 'trade secret'.

Explicit confidentiality clauses and agreements can effectively protect your business from misappropriation of your confidential information or trade secrets.

The Guide will elaborate more on this in **Section 3**.

### 2.3 Breach of obligation of confidentiality

Lastly, this obligation of confidentiality must have been breached, i.e., the confidential information/trade secret was used, disclosed and/or taken.

This will entitle you to claim remedies in compensation for the misappropriation of your information/trade secret (see **Section 2.5** below for more details).

Typically, this obligation will be considered breached where a person has used and/or disclosed your company's information/trade secrets to the detriment of your company.

#### Real-world case study

- A distributor, Adinop Co Ltd, had an agreement to give quarterly reports containing important customer information to Rovithai Ltd, its supplier. This information was for the clear purpose of assisting and supporting Adinop to develop the market for its products.
- When their business relationship ended, Rovithai misused this customer information to inform Adinop's customers that it was no longer Rovithai's distributor. This caused Adinop to lose 5 key customers.
- The Court found that the use of the customer information for purposes other than that for which it had been provided amounted to a breach in the obligation of confidence.

For more details, see [https://www.elitigation.sg/gdviewer/s/2019\\_SGCA\\_67](https://www.elitigation.sg/gdviewer/s/2019_SGCA_67)

What happens in cases where your company's confidential information/trade secrets have been taken without your permission but have not yet been misused, disclosed or relied upon?

- The courts have recognised that as modern technology has advanced, it is significantly easier to access, copy and disseminate vast amounts of confidential information almost instantaneously. While your company may not have suffered a monetary 'loss' from the unauthorised taking of the information, the information itself could lose its confidential nature.
- As such, to protect companies, the law presumes that this obligation of confidence has been breached unless the 'taker' of the information can show that his conscience was not affected by the taking of the information.

#### Real-world case study

- Two ex-employees from I-Admin, a company dealing in administrative data processing services, accessed, downloaded and circulated confidential materials from I-Admin which they knew to be confidential in nature.
- These materials were specifically acquired to be reviewed and potentially used for the benefit of a competitor company which the ex-employees had set up after leaving the employ of I-Admin. Ultimately, however, it was not proven that I-Admin's confidential materials were relied on for the creation of the source codes, systems and materials for the competitor company.
- Despite this lack of 'use' of I-Admin's confidential materials, the court found that the obligation of confidence had still been breached on the basis that the materials had been acquired, circulated and referenced without permission. The ex-employees, who knew that the information they were acquiring was confidential, could not displace the presumption that their conscience were negatively affected.

For more details, see [https://www.elitigation.sg/gd/s/2020\\_SGCA\\_32](https://www.elitigation.sg/gd/s/2020_SGCA_32)



## 2.4 Exceptions

In exceptional cases, the recipient or taker of the information may be able to justify its disclosure of your confidential information as it is in the public interest to do so.

- **Example:** The Defendant obtained confidential information through the course of arbitration proceedings with the Plaintiffs which suggested that the Plaintiffs were involved in criminal wrongdoing. This information was then disclosed to the Police for further investigation. The court held that disclosure to the proper authorities where there is reasonable suspicion of criminal conduct was an exception to the obligation of confidence, and the Defendant was found not to be liable for breach of confidence. For more details, see [https://www.elitigation.sg/gdviewer/s/2009\\_SGHC\\_142](https://www.elitigation.sg/gdviewer/s/2009_SGHC_142).
- **Example:** Technicians who had left the employ of the Plaintiff laboratory disclosed the Plaintiff's confidential information to a newspaper. The information proved that the Plaintiff's breath analysers (which had been authorised for use by the police) produced inaccurate readings. While the court recognised that the Plaintiff had the right to protect their own internal, confidential documents, publication of the information in the newspaper was allowed as members of the public could potentially be convicted of drink driving on the basis of those readings. For more details, see <https://www.ucpi.org.uk/wp-content/uploads/2018/03/Lion-Laboratories-Ltd.-v-Evans-1985-Q.B.-526-CA.pdf>.

## 2.5 Remedies

Various remedies are available once breach of confidence has been established, including:

Remedy	What it is
Injunction	Generally, an injunction prevents the other party from doing an act. In cases involving trade secrets, an injunction typically prevents the other party from further disclosure, dissemination or use of the trade secret.
Monetary compensation	Monetary compensation generally takes the following forms: <ul style="list-style-type: none"><li>■ <b>Damages:</b> a sum to compensate you for your loss;</li><li>■ <b>Account of Profits:</b> a sum representing the total profit the other party has gained from the use/disclosure of your trade secrets.</li></ul>
Order for delivery-up or destruction	If the other party has copies or other records of your trade secrets and/or confidential information, the court may order these copies to be handed over to you or destroyed, depending on your preference.

# 3. PROTECTION AND MANAGEMENT OF TRADE SECRETS

---

In this section, the Guide will cover the following:

- A general framework to manage and protect your trade secrets; and
- Factors to consider when drafting non-disclosure agreements and/or confidentiality clauses.

## Steps to manage and protect your trade secrets

The four steps below provide a general framework for the management and protection of your trade secrets.



### 3.1 Identify your trade secrets

To effectively protect your trade secrets, you have to know what qualifies as a trade secret.

#### Checklist

- Has this information been kept secret, or out of the public domain?  
[For instance, is this information only accessible by select employees and/or customers?]
- Is this information commercially valuable to the business?  
[For instance, does the business rely on this information in order to derive profits? Would other businesses pay to buy/ access this information?]
- Would it be difficult to reverse engineer or re-create the trade secret?
- Is there a process to identify trade secrets on an ongoing basis?

### 3.2 Record and review your trade secrets

After identifying your trade secrets, it is important to record them and update your record of trade secrets periodically.

#### Checklist

- Is there a record of all the trade secrets owned or used by the company? Consider:
  - The different categories of trade secrets your company may own – which ones are more valuable and may need additional protection?
  - Keeping records of trade secrets (i) disclosed to third parties during the course of a business relationship and (ii) licenced for your use by third parties
- Are there details of the trade secret? For instance, consider including:
  - What the trade secret covers;
  - How the trade secret can be used or is currently being used;
  - Who developed the trade secret; and
  - When the trade secret was developed.
- Are your trade secret records updated? Consider conducting reviews of your trade secret records monthly, quarterly or yearly to ensure that the records are up-to-date.

#### Case Study

Founded in 2014, Cynopsis Solutions offers regulatory technology (RegTech) solutions which digitises and automates compliance and regulatory processes. Cynopsis uses a nimble multi-pronged approach towards protecting their various intangible assets, which include trade secrets. To protect its trade secrets, Cynopsis uses confidentiality clauses and repository services; and also applies security controls to prevent unauthorized access to company information. Today, Cynopsis meets the international standards for information security (ISO/IEC 270001:2013 certified), which cover three key dimensions – Confidentiality, Integrity and Availability.

Cynopsis' robust trade secrets protection helped it to secure its competitive edge, and gain the trust and confidence of its clients – which were critical in driving business growth and market expansion.



**As a RegTech company that develops proprietary software solutions, it was not always suitable for patent protection as there are considerations like cost and speed to market.**

Therefore, Cynopsis Solutions decided to use other approaches to protect our intangible assets. With the strong safeguards in place to protect our trade secrets, we have met international standards for information security.

This has given us the confidence to expand our business into global markets like UK and US.

**Mr Chionh Chye Kit,**  
CEO & Co-Founder,  
Cynopsis Solutions Pte Ltd

Please visit our Trade Secrets page for more case studies.



<https://www.ipos.gov.sg/about-ip/trade-secrets>

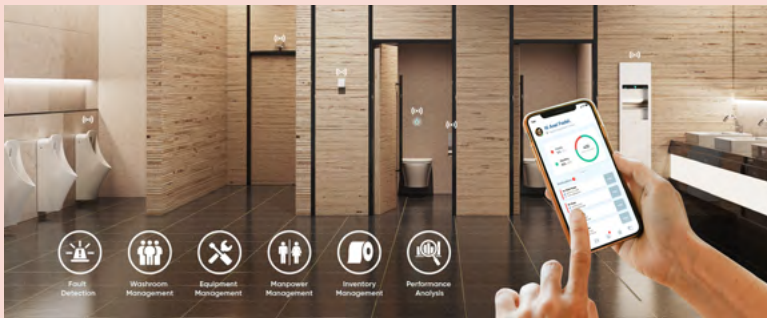
### 3.3 Securing your trade secrets

Consider putting in place the following measures to protect your trade secrets:

#### Checklist

- Are your trade secrets marked “HIGHLY CONFIDENTIAL” or “SECRET”, and/or contain any notices of confidentiality to inform the reader that the document is highly confidential in nature?
- Is the document protected through cybersecurity measures? These include:
  - File locking measures e.g. password protection, encryption; and
  - Anti-virus and firewall protection.
- Is the document protected through physical controls? These include:
  - Restricting access to your office to authorised personnel using key-cards;
  - Prohibiting the use of cameras, external storage devices or recording devices in areas containing trade secrets;
  - Creating a logbook where persons accessing the trade secret must sign in and out.
- If trade secrets need to be disclosed or accessed, have the relevant agreements containing confidentiality obligations been signed? These include:
  - Non-disclosure agreements
  - Employment contracts

#### Case Study



Rigel is a company known for its innovative, eco-friendly, and smart sanitary solutions. Behind its innovations, Rigel has a rich intellectual property (IP) portfolio of close to 30 trade marks, patents, registered designs, and other non-registrable IP and intangible assets (IA) such as trade secrets and confidential information.

To protect its non-registrable IP and IA, measures such as the use of confidentiality clauses, restricting access to shared drive, and classification of documents and emails were taken. The importance of these measures was highlighted when a former employee leaked out confidential product information to a competitor, and legal action had to be taken. The robust protective measures in place to safeguard its trade secrets has supported Rigel’s entry and expansion into over 35 markets globally.



We became more aware about the importance of protecting our intellectual property after experiencing trade secret misappropriation by a former employee, when classified information on one of our products was leaked to a competitor.

Although we were able to take legal action, we learned from our legal partners that this could have been prevented with stronger measures to protect our trade secrets.



**Mr Christopher Ng,**  
Group CEO,  
Rigel Technology (S) Pte Ltd

Please visit our Trade Secrets page for more case studies.



<https://www.ipos.gov.sg/about-ip/trade-secrets>

### 3.4 Employee training and education on trade secrets

Employees and former employees are persons who may have access to your trade secrets, and this gives rise to high risks of trade secret theft or misuse. As such, it is important to train employees on the importance of trade secret confidentiality.

#### Checklist

- Have employees been trained on recognising trade secrets and confidential information?
- Is there a trade secret policy that employees can refer to, to remind them of their obligations of confidentiality?
- Are employees required to agree in writing to (i) confidentiality agreements and/or (ii) non-compete agreements with respect to trade secrets?
- Are employees required to agree in writing that they do not own trade secrets/other forms of IP that they may develop in the course of their employment? And that ownership of all such IP vests with the company?
- Have employees been trained on physical measures to protect trade secrets? These include:
  - Locking areas in the office containing trade secrets;
  - Destroying unrequired copies of sensitive documents containing trade secrets; and
  - Not leaving documents containing trade secrets in plain view or in public.
- Have employees been trained on cybersecurity practices to prevent trade secret leaks? These include:
  - Identifying phishing e-mails and suspicious links
  - Clearing of metadata when sending documents to third parties
  - Prohibiting the use of personal email addresses to send work-related e-mails
- Are there exit interviews in place for departing employees? These should remind employees:
  - That their obligation to keep your trade secrets confidential remains even after the employee leaves your company
  - To return all confidential information in his/her possession to the company
  - That your company may take legal action against the employee or his/her future employer if any of your trade secrets are stolen and misused by the employee or his/her future employer
- Have employees been instructed to obtain clearance for activities which might disclose your trade secrets to the public? Such activities include:
  - Conducting workshops or talks with third-parties
  - Publishing technical papers
  - Demonstrations of your company's product or process to third-parties

## Non-disclosure agreements and confidentiality clauses

Consider the following when preparing non-disclosure agreements and confidentiality clauses:

S/N	Issue	Points to Consider
1)	Parties	<ul style="list-style-type: none"> <li><input type="checkbox"/> Identify the parties with precision.</li> <li><input type="checkbox"/> Identify who the recipient of information can disclose the information to. This may include employees, subsidiaries or professional advisors.</li> </ul>
2)	Definition of "trade secret"	<ul style="list-style-type: none"> <li><input type="checkbox"/> Clearly define the trade secret.</li> <li><input type="checkbox"/> Consider expanding the definition of "trade secrets" to cover derivative information created through use of the trade secret.</li> </ul>
3)	Purpose	<ul style="list-style-type: none"> <li><input type="checkbox"/> The agreement should limit how the recipient of trade secret information can use such information.</li> </ul>
4)	Non-disclosure obligations	<ul style="list-style-type: none"> <li><input type="checkbox"/> The agreement should include a duty on the recipient to safeguard and protect your trade secrets.</li> <li><input type="checkbox"/> Consider including specific obligations on the recipient, such as implementing security measures and providing notice to you on security breaches.</li> </ul>
5)	Return or destruction of trade secret information	<ul style="list-style-type: none"> <li><input type="checkbox"/> The recipient should be obligated to return or destroy the disclosed information once the Purpose of the Agreement has come to an end.</li> <li><input type="checkbox"/> Consider including a provision to enable the destruction or return of information at any time, upon your request.</li> </ul>
6)	Ownership	<ul style="list-style-type: none"> <li><input type="checkbox"/> Clearly state that you retain all rights, titles or interests to the trade secret information being disclosed.</li> <li><input type="checkbox"/> Clearly state that the non-disclosure agreement does not constitute a grant of any assignment or licence of trade secret information to the recipient.</li> </ul>

### Sample confidentiality clause (Simple)

1. The parties agree that the terms of this agreement are confidential, and not to disclose the same to any person except as expressly permitted in this clause.
2. [Employee/Third party] undertakes that they shall not at any time during this agreement, and for a period of [three] years after termination or expiry of this agreement, disclose to any person any confidential information concerning the business affairs, customers, clients or suppliers of the Company or of any member of the group of companies to which the Company belongs, except as expressly permitted in this clause.
3. Neither party shall use any other party's confidential information for any purpose other than to exercise its rights and perform its obligations under or in connection with this agreement.

A longer form non-disclosure agreement may be found at **Annex A** of the Guide.

# 4. COMMERCIALISATION AND EXPLOITATION OF TRADE SECRETS

In this section, the Guide will cover the ways you can commercialise and exploit your trade secrets.

## 4.1 Licensing your trade secret

In a trade secret licence, you (the licensor) give a third party (licensee) the permission to use your trade secret in exchange for compensation. The trade secret will still belong to you, but you will be able to receive royalties from the licensee's use of the trade secrets.

- **Example:** Franchise agreements often include trade secret licences. This allows corporations such as McDonalds, GNC and Anytime Fitness to expand their operations worldwide.

Consider the following issues when licensing your trade secret:

Issue	Points to Consider
Degree of exclusivity	<p>This affects who will be able to exploit your trade secrets.</p> <ul style="list-style-type: none"> <li>■ <b>Exclusive licence:</b> the licensee can exploit the trade secret to the exclusion of all persons, including the licensor, unless there are express carve-outs.</li> <li>■ <b>Sole licence:</b> means an exclusive licence where the licensor also reserves the right to exploit the trade secret. The licensor is precluded from granting further licenses to any other party.</li> <li>■ <b>Non-exclusive licence:</b> the licensee is granted the right to use the trade secret, but the licensor remains free to use the trade secret and to grant licenses to any number of licensees to exploit the trade secret.</li> </ul>
Payment terms	<p>To consider the frequency and determination of payment, e.g., percentage of licensee's profits, fixed licence fee, one-time lump sum.</p>
Maintaining control over secrecy	<p>Licensor should require the licensee to maintain the secrecy of the trade secret.</p> <p>Practically, this may mean providing for:</p> <ul style="list-style-type: none"> <li>■ <b>Audit rights:</b> the right for the licensor to inspect the licensee's records and measures to check if the licensee is complying with the terms.</li> <li>■ <b>Survival clauses:</b> the maintenance of the secrecy of the trade secret even after the term/termination of the agreement. <ul style="list-style-type: none"> <li>● <b>Example:</b> Notwithstanding any expiration or termination of this Agreement, clauses [insert clauses pertaining to maintenance of secrecy] shall survive this Agreement under the terms hereof for a period of three (3) years beyond the termination or expiration hereof.</li> </ul> </li> <li>■ <b>Access rather than disclosure:</b> to protect the secrecy of the trade secret, consider only granting access to the trade secret rather than providing full details of the trade secret. <ul style="list-style-type: none"> <li>● <b>Example:</b> A restaurant may allow its franchisees to use its special spice mixes and sauces, but not to know the ingredients/formula of these mixes.</li> </ul> </li> </ul>

## 4.2 Assignment of trade secrets

The ownership of the trade secret may also be transferred or 'assigned' to another party in exchange for compensation. As such, you are able to treat trade secrets like assets which can be bought or sold. Once the trade secret has been sold, it will no longer belong to the seller (the 'assignor'), but to the buyer (the 'assignee').

When trade secrets are assigned, the seller of the trade secret will generally be required to not disclose the trade secret, and will owe the buyer strict duties to maintain confidentiality of the trade secret. Otherwise, the value of the trade secret can easily be diminished by the seller after he has received compensation for the selling of the trade secret.

## 4.3 Using your trade secrets as part of a joint venture or collaboration

Companies may also disclose or share their trade secrets with each other through joint ventures or business collaborations. This may allow companies to jointly develop new products or services more efficiently.

A well-drafted non-disclosure agreement is crucial in these collaborations. Consider:

- Carefully identifying each party's trade secrets to define the scope of protection before the venture/collaboration begins (e.g., Clause 2 in Annex A).
- Defining the scope of use of the trade secrets for the purposes of the joint venture (e.g., defining the Purpose, see Clause 3 in Annex A).
- Defining which individuals from each respective entity will have access to the trade secrets, and how the trade secrets may be shared (e.g., Clause 4 in Annex A).

### Case Study



Singapore-based Nutrition Technologies is revolutionising the agriculture sector by turning predominantly wasted by-products and Black Soldier Fly larvae into valuable products such as organic fertilisers, protein, and oil.

To protect their trade secrets, such as customer information and proprietary chemical formulae, Nutrition Technologies has used confidentiality agreements and cataloguing service. It has also used Tangibly, a trade secret management platform.

Our founders have a strong passion for sustainability and changing the way the world feeds itself. We recognise the importance of securing our competitive edge by protecting our technology and confidential information.

We have used Tangibly to help us better track and manage its trade secrets and ensure our key business and operational processes are effectively safeguarded. This has allowed us to build a strong base for our business expansion.

**Mr Martin Zorrilla,**  
Chief Technology Officer,  
Nutrition Technologies Pte Ltd

Please visit our Trade Secrets page for more case studies.














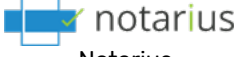
<https://www.ipos.gov.sg/about-ip/trade-secrets>



# 5. TOOLS AND SERVICES FOR TRADE SECRET PROTECTION, MANAGEMENT AND USE

Various tools and services can be used to protect, manage and use your trade secrets effectively. Some examples of these tools and services include.

Tool/Service	Service providers	Features
VPN and Firewalls	 GlobalProtect	<ul style="list-style-type: none"> <li>Remote access VPN services that provide secure access to internal and cloud-based business applications.</li> <li>URL filtering services which filter access to malicious domains</li> </ul>
	 Perimeter 81	<ul style="list-style-type: none"> <li>Activates VPN protection automatically when users connect to unknown and untrusted networks</li> <li>Provides high-speed, private servers with dedicated IP addresses</li> </ul>
	 NordLayer	<ul style="list-style-type: none"> <li>Provides network segmentation to create private gateways, enabling admins to segment local networks and restrict data to selected users</li> <li>Allows for whitelisting of Internet Protocol (IP) addresses, which can help to control user access to data and applications on a network</li> </ul>
Trade Secret Management tools	 Tangibly	<ul style="list-style-type: none"> <li>Helps businesses track and manage non-disclosure agreements, as well as limit access to trade secrets on a need-to-know basis.</li> </ul>
	 Decipher	<ul style="list-style-type: none"> <li>Easy-to-use software system for organizing and securely storing trade secrets, accelerating innovation, gaining insights into your portfolio, and more effectively leveraging your intellectual assets.</li> </ul>
	 AWS Secrets Manager	<ul style="list-style-type: none"> <li>Secures secrets by encrypting them with encryption keys</li> <li>Integrates with AWS' logging and monitoring services for centralized auditing</li> <li>Access to secrets can be managed using AWS identity and access management policies and resource-based policies.</li> </ul>

Tool/Service	Service providers	Features
Encryption services	 Vitrium	<ul style="list-style-type: none"> <li>Provides digital rights management controls to prevent printing, copying or downloading of files.</li> <li>User access controls to assign or revoke user access to sensitive information.</li> <li>Tracking and analytics data to identify who is accessing your content, when, and from what device and IP address.</li> </ul>
	 ESET	<ul style="list-style-type: none"> <li>Provides a range of features to prevent and detect cybersecurity threats, such as full disk encryption services which protect users against loss or theft of data</li> </ul>
Repository services	 AON	<ul style="list-style-type: none"> <li>Allows businesses to register their trade secrets on a blockchain register. These blockchain records serve as a verifiable record of the trade secret document, which can be used to demonstrate your ownership of the trade secret.</li> </ul>
	 SQL View	<ul style="list-style-type: none"> <li>Secures email records and attachments automatically</li> <li>Automatically tracks retention period of records; prompts user to archive or dispose records when it is time to do so.</li> </ul>
Time-stamping services	 Entrust	<ul style="list-style-type: none"> <li>Provides timestamps on documents, which can be used to guarantee the existence of a document or transaction from the exact date and time of the timestamp.</li> </ul>
	 Notarius	<ul style="list-style-type: none"> <li>Adds a timestamp token to electronic documents, certifying the content of the document at the exact time, to the nearest second</li> </ul>

# ACKNOWLEDGEMENT

---

We would like to extend our appreciation to our partners – Action Community for Entrepreneurship, Enterprise Singapore, SGTech, SBF, and Singapore FinTech Association, who have provided us with useful feedback for this Guide.

We would also like to thank Bird & Bird ATMD LLP whom we commissioned to prepare this Guide.

For all who contributed, this Guide would not have been possible without your valuable input. We look forward to working closely with you and the community to continue supporting enterprises in the protection and management of trade secrets as we compete globally in this era of rapid technological advancements.

Copyright © 2022 Intellectual Property Office of Singapore

You may download, view, print and reproduce this document without modifications, but only for non-commercial use. All other rights are reserved.

## **ANNEX A – SAMPLE NON-DISCLOSURE AGREEMENT**

This agreement is dated [DATE]

### **Parties**

- (1) [FULL COMPANY NAME] incorporated and registered in [COUNTRY] with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS]  
**(Discloser)**
- (2) [FULL COMPANY NAME] incorporated and registered in [COUNTRY] with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS]  
**(Recipient)**

(each a “**Party**” and collectively the “**Parties**”)

### **BACKGROUND**

- (A) The Parties intend to enter into discussions relating to the Purpose which will involve the disclosure of confidential information from Discloser to Recipient.
- (B) The Parties have agreed to comply with this agreement in connection with the disclosure and use of Confidential Information.

### **Agreed terms**

#### **1. Interpretation**

##### **1.1 Definitions:**

**Business Day:** a day other than a Saturday, Sunday or public holiday in Singapore when banks in Singapore are open for business.

**Confidential Information:** has the meaning given in clause 2.

**[Group:** in relation to a company, that company, any subsidiary or holding company from time to time of that company, and any subsidiary from time to time of a holding company of that company. Each company in a Group is a member of the Group.]

**[Group Company:** in relation to a company, any member of its Group.]

**Purpose:** [STATE THE PURPOSE, FOR EXAMPLE, THE EVALUATION OR ESTABLISHMENT OF A COLLABORATION IN RESPECT OF A PARTICULAR PROJECT].

**Representative(s):** in relation to each party [and any member of its Group]:

- a) its officers and employees that need to know the Confidential Information for the Purpose;

- b) its professional advisers or consultants who are engaged to advise that party [and/or any member of its Group] in connection with the Purpose;
- c) its contractors and sub-contractors engaged by that party [and/or any member of its Group] in connection with the Purpose; and
- d) any other person to whom the other party agrees in writing that Confidential Information may be disclosed in connection with the Purpose.

[Note: Where trade secret(s) are involved, the list of Representative(s) should be restricted to safeguard the secrecy of the trade secret(s)]

## 2. Confidential Information

2.1 **Confidential Information** means all confidential information relating to the Purpose which Discloser or its Representatives [or any of its Group Companies, or their Representatives] directly or indirectly discloses, or makes available, to Recipient or its Representatives [or any of its Group Companies, or their Representatives][, before, on or after the date of this agreement]. This includes:

- (a) the fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations;
- (b) [the [existence and] terms of this agreement;]
- (c) all confidential or proprietary information relating to:
  - (i) the business, assets, affairs, customers, clients, suppliers[, **OR** or] plans[, intentions, or market opportunities] of Discloser [or of any of Discloser's Group Companies]; and
  - (ii) the operations, processes, product information, know-how, technical information, designs, trade secrets or software of Discloser [, or of any of Discloser's Group Companies];
- (d) any information, findings, data or analysis derived from Confidential Information; [and]
- (e) any other information that is identified as being of a confidential or proprietary nature [; and **OR** .]

but excludes any information referred to in clause 2.2.

2.2 Information is not Confidential Information if:

- (a) it is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by Recipient or its Representatives [or by any of Recipient's Group Companies or their Representatives] in breach of this agreement [(except that any compilation of otherwise public information in a form not publicly known shall still be treated as Confidential Information)];
- (b) it was available to Recipient on a non-confidential basis prior to disclosure by Discloser;

- (c) it was, is, or becomes available to Recipient on a non-confidential basis from a person who, to Recipient 's knowledge, is not under any confidentiality obligation in respect of that information;
- (d) it was lawfully in the possession of Recipient before the information was disclosed by Discloser; [and]
- (e) [it is developed by or for Recipient independently of the information disclosed by Discloser [and Recipient provides documentary evidence of such independence to the reasonable satisfaction of Discloser]; and]
- (f) the Parties agree in writing that the information is not confidential.

**3. Confidentiality obligations**

3.1 In return for Discloser making Confidential Information available to Recipient, Recipient undertakes to Discloser that it shall:

- (a) keep the Confidential Information secret and confidential;
- (b) not use or exploit the Confidential Information in any way except for the Purpose;
- (c) not directly or indirectly disclose or make available any Confidential Information in whole or in part to any person, except as expressly permitted by, and in accordance with this agreement;
- (d) establish and maintain adequate security measures (including any reasonable security measures proposed by Discloser from time to time) to safeguard the Confidential Information from unauthorised access or use.
- (e) [INCLUDE ANY OTHER SPECIFIC REQUIREMENTS.]

**4. Permitted disclosure**

4.1 The Recipient undertakes not to disclose the Confidential Information to any person or body, except to the following:

Name	Designation and Company Name

4.2 The Recipient may with express and written consent of the Discloser include additional Representatives to whom the Confidential Documentation may be disclosed. Such disclosure shall be made only to the extent necessary to carry out the Purpose, and any such disclosure shall be made in such manner as to ensure that any such Representative shall comply with the terms of this Agreement as if they were the

Recipient. The Recipient shall be responsible for any breach of this Agreement by any of its Representatives.

## **5. Mandatory disclosure**

5.1 Subject to the provisions of this clause 5, Recipient may disclose Confidential Information to the minimum extent required by:

- (a) an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction;
- (b) the rules of any listing authority or stock exchange on which its shares are listed or traded; or
- (c) the laws or regulations of any country to which its affairs are subject.

5.2 Before Recipient discloses any Confidential Information pursuant to clause 5.1 it shall, to the extent permitted by law, give Discloser as much notice of this disclosure as possible. Where notice of such disclosure is not prohibited and is given in accordance with clause 5.2, Recipient shall take into account Discloser's requests in relation to the content of this disclosure.

5.3 If Recipient is unable to inform Discloser before Confidential Information is disclosed pursuant to clause 5.1 it shall, to the extent permitted by law, inform Discloser of the full circumstances of the disclosure and the information that has been disclosed as soon as reasonably practicable after such disclosure has been made.

## **6. Return or destruction of Confidential Information**

6.1 If so requested by Discloser at any time by notice in writing to Recipient, Recipient shall promptly:

- (a) destroy or return to Discloser all documents and materials (and any copies) containing, reflecting, incorporating or based on Discloser's Confidential Information;
- (b) erase all the Confidential Information from its computer and communications systems and devices used by it, or which is stored in electronic form; [and]
- (c) [[to the extent technically and legally practicable,] erase all the Confidential Information which is stored in electronic form on systems and data storage services provided by third parties; and]
- (d) certify in writing to Discloser that it has complied with the requirements of this clause 6.1.

6.2 Nothing in clause 6.1 shall require Recipient to return or destroy any documents and materials containing or based on the Confidential Information that Recipient is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or the rules of any listing authority or stock exchange,

to which it is subject. The provisions of this agreement shall continue to apply to any documents and materials retained by Recipient pursuant to this clause 6.2.

## **7. Reservation of rights and acknowledgement**

- 7.1 Discloser reserves all rights in its Confidential Information. The disclosure of Confidential Information by Discloser to Recipient does not give Recipient or any other person any licence or other right in respect of any Confidential Information beyond the rights expressly set out in this agreement.
- 7.2 Except as expressly stated in this agreement, Discloser makes no express or implied warranty or representation concerning its Confidential Information, including but not limited to the accuracy or completeness of the Confidential Information.
- 7.3 The disclosure of Confidential Information by Discloser shall not form any offer by, or representation or warranty on the part of, Discloser to enter into any further agreement with Recipient [in relation to the Purpose or the development or supply of any products or services to which the Confidential Information relates to].

## **8. Indemnity**

- 8.1 Recipient shall indemnify Discloser [and each member of its Group (each an Indemnified Person)] against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other [reasonable] professional costs and expenses) suffered or incurred by [Discloser **OR** each Indemnified Person] arising out of or in connection with any breach of this agreement by Recipient, including as a result of the actions or omissions of any of its Representatives in accordance with clause 4.2.
- 8.2 If a payment due from Recipient under clause 8.1 is subject to tax (whether by way of direct assessment or withholding at its source), the [Discloser **OR** Indemnified Person] shall be entitled to receive from Recipient such amount as shall ensure that the net receipt, after tax, of the [Discloser **OR** Indemnified Person] in respect of the payment is the same as it would have been were the payment not subject to tax.

## **9. Inadequacy of damages**

Without prejudice to any other rights or remedies that Discloser may have, Recipient acknowledges and agrees that damages alone would not be an adequate remedy for any breach of the terms of this agreement. Accordingly, Discloser shall be entitled to the remedies of injunctions, specific performance or other equitable relief for any threatened or actual breach of this agreement by Recipient.



## 10. General

10.1 **Assignment and other dealings.** The Parties' rights and obligations under this Agreement, [including the rights and obligations of the Parties' Group Companies] will bind and inure to the benefits of their respective successors, heirs, executors, and administrators and permitted assigns. Neither Party shall assign or delegate its rights and obligations under this Agreement either in whole or in part without the prior written consent of the other Party.

### 10.2 Entire agreement.

- (a) This agreement constitutes the entire agreement between the Parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.
- (b) Each party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this agreement. Each party agrees that it shall have no claim for innocent or negligent misrepresentation [or negligent misstatement] based on any statement in this agreement.

10.3 **Variation.** No variation of this agreement shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

10.4 **Waiver.** No failure or delay by a party to exercise any right or remedy provided under this agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

### 10.5 Severance

- (a) If any provision or part-provision of this agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this agreement.
- (b) If any provision or part-provision of this agreement is deemed deleted under clause 10.5(a), the Parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

10.6 **Counterparts.** This Agreement may be executed in several counterparts, all of which together shall constitute one agreement binding on all Parties hereto, notwithstanding that all the Parties have not signed the same counterpart. The Parties agree that this Agreement may be exchanged by facsimile, pdf or other electronic means, which upon request of a Party shall be followed up with originals.

10.7 **Third party rights.** [Unless it expressly states otherwise,] this agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 2001 to enforce any term of this agreement.

10.8 **Governing Law and Jurisdiction.**<sup>1</sup> This Agreement shall be governed in accordance with the laws of Singapore and the Courts of Singapore shall have exclusive jurisdiction over any dispute arising out of this Agreement.

This agreement has been entered into on the date stated at the beginning of it.

Signed by [NAME OF DIRECTOR] for and on behalf of [NAME OF DISCLOSER]	..... Director
Signed by [NAME OF DIRECTOR] for and on behalf of [NAME OF RECIPIENT]	..... Director

---

<sup>1</sup> Alternative dispute resolution (ADR), such as mediation or arbitration, may be considered, and relevant dispute resolution clauses may be included into non-disclosure agreements to introduce ADR into the parties' dispute resolution process. In some cases, ADR might even be more efficacious (e.g. technically complex matters).

You may refer to the following webpage for more information on dispute resolution:  
<https://www.ipos.gov.sg/manage-ip/resolve-ip-disputes>.

You should approach a legal professional if you require legal advice; legal professionals will also be able to assist in recommending and drafting suitable dispute resolution clauses to suit the needs in a matter.

The Intellectual Property Office of Singapore (IPOS) is the national authority that registers and is responsible for the administration of IP rights in Singapore. IPOS helps businesses use IP and intangible assets (IA) to grow and is committed to building Singapore into an international IA/IP hub. IPOS is a statutory board under the Ministry of Law.

Published September 2022  
© Intellectual Property Office of Singapore

You are free to copy, publish, distribute, and transmit this publication, unmodified and in its entirety only, for non-commercial purposes. All other rights reserved.