《幕簾協議》

(I) 目錄

(II) 管理框架和原則

A. 序言

《幕簾協議》的制定是為了在數字時代確保個人數據的隱私保護和合理使用。隨著數據處理量的不斷增加，個人和組織面臨著更多的挑戰和責任，需要確保數據的安全性和透明度。該協議的目的是為內部提供明確的指導原則，以確保數據處理符合合規和道德標準。

在這個協議中，我們旨在強調個人數據隱私的重要性，並確保個人信息不會被不當使用、洩露或濫用。我們希望通過建立明確的規則和流程，為個人和組織提供保護和控制個人數據的機制。

同時，我們也鼓勵適當的數據分享和合作，以支持組織內部的有效運作和創新。我們認識到數據共享可以帶來許多好處，但也必須在合規的框架下進行，確保數據的安全性和合法性。

為了更好地管理和共享數據，並保護數據的安全性，我們建立了一個不同機密等級的分類系統。這將幫助個人和組織瞭解數據的敏感性，並採取適當的措施進行保護和控制。

最後，我們強調個人的責任和自主權，個人有權決定自己數據的使用和訪問。我們鼓勵個人積極參與數據處理的決策過程，並確保他們對自己數據的掌控和保護。

《幕簾協議》這個名字的選擇是寓意著數據處理和隱私保護之間的平衡。幕簾作為一種遮蔽視線的物件，象徵著對數據的保密和隱私保護。同時，幕簾也象徵著透明度和開放性，使數據處理的過程能夠被合法和有權的人所知悉。這個名字旨在傳達在保護隱私的同時，確保數據處理的合規和合理性的理念。

通過遵守《幕簾協議》，我們相信個人和組織能夠更好地處理和保護數據，確保數據的合理使用和隱私的安全。只有通過共同努力，我們才能在數字時代建立可持續發展的數據處理和隱私保護的框架。

B. 背景

在數字時代，個人和組織處理的數據量不斷增加，數據的處理和隱私保護變得至關重要。隨著技術的進步和信息的普及，個人數據的收集、存儲和使用已成為常態。與此同時，隱私保護和合理使用數據的問題也日益引起關注。

個人數據的隱私洩露可能導致個人權益受損、信任破壞以及潛在的濫用風險。此外，組織在處理大量數據時，也面臨著數據安全性、合規性和聲譽風險等挑戰。因此，建立一套明確的指導原則和規範，以確保數據的適當使用和保護，成為當務之急。

《幕簾協議》的制定目的就是為了規範內部數據處理和隱私保護的行為，確保個人和組織在處理數據時遵守合規和道德標準。該協議的出台旨在為個人和組織提供一個框架，明確數據處理的准則和原則，以及保護個人隱私的措施和要求。

在制定《幕簾協議》時，需要考慮到不同級別的數據敏感性和訪問權限，制定相應的控制措施和限制規定。例如，將數據分為不同的級別，根據級別確定人員的訪問權限，確保只有授權人員能夠訪問和處理相應級別的數據。

此外，協議的制定還需要注重數據的合理使用和分享。數據的適當分享和合作可以促進組織內部的有效運作和創新，但同時也需要遵守合規的原則，確保數據的安全性和合法性。

通過制定《幕簾協議》，個人和組織可以更好地理解數據處理和隱私保護的重要性，明確自身的責任和義務，並採取相應的措施來保護數據的隱私和安全。只有在保護個人隱私的同時，合理使用和保護數據，才能在數字時代建立信任和可持續發展的數據處理體系。

C. 定立目的

1. 提供內部對於數據處理（隱私）的明確指導：《幕簾協議》的目的是為內部提供明確的指導原則，確保個人和組織在處理數據時遵守合規和道德標準。協議將明確規定數據處理的原則、流程和規範，為內部成員提供指引，以確保他們在數據處理中的行為符合合規要求。

2. 保護個人數據的隱私權：協議的目的之一是確保個人資料的隱私不受到不當使用、洩露或濫用。通過制定明確的隱私保護措施和要求，協議將確保個人數據得到妥善保護，防止未經授權的訪問和濫用，保護個人隱私權益。

3. 促進數據的適當分享與合作：協議鼓勵適當的數據分享和合作，以支持組織內部的有效運作和創新。通過明確合規框架和規定，協議將幫助組織在數據分享和合作中確保數據的安全性和合法性，促進信息共享和協同工作，從而提升組織的效率和創新能力。

4. 建立不同機密等級的分類系統：為了更好地管理和共享數據，並保護數據的安全性，協議建立了一個不同機密等級的分類系統。該系統將幫助個人和組織瞭解數據的敏感性，並根據不同等級確定數據的訪問權限和控制措施，確保數據得到適當的保護和控制。

5. 強調個人責任和自主權：協議強調個人對於自身數據的責任和自主權。個人有權決定自己數據的使用和訪問，並可以積極參與數據處理的決策過程。協議將鼓勵個人行使自主權，確保他們對自己數據的掌控和保護，同時也需要履行相應的責任，遵守合規要求和隱私保護措施。

D. 名字由來

《幕簾協議》這個名字的由來寓意著數據處理與隱私保護之間的透明度和保密性的平衡。幕簾作為一種遮蔽視線的物件，象徵著對於數據的保密和隱私保護。同時，幕簾也象徵著透明度和開放性，使得數據處理的過程能夠被合法和有權的人所知悉。這個名字旨在傳達在保護隱私的同時，確保數據處理的合規和合理性的理念。

具體來說，這個名字的來源可以解讀為以下幾個方面：

1. 保密性與隱私保護：幕簾作為一種遮蔽物，象徵著對於數據的保密和隱私保護。它象徵著將數據保護在幕簾後，防止未經授權的訪問和洩露。名字中的「幕簾」一詞強調了對於個人隱私的重視和保護。

2. 透明度與開放性：幕簾同時也具有透明度和開放性的意味。在數據處理的過程中，透明度是指合法和有權的人能夠瞭解和知悉數據的處理過程。這種透明度有助於建立信任和合規性。名字中的「幕簾」一詞暗示了數據處理應該在透明和開放的基礎上進行。

3. 平衡與合理性：名字中的「幕簾」一詞傳達了在數據處理與隱私保護之間尋求平衡的理念。數據處理需要在保護個人隱私的前提下，遵守合規和合理性的原則。幕簾作為一個符號，表示了在保護隱私的同時，確保數據處理的合規和合理性的平衡。

綜上所述，《幕簾協議》這個名字的由來寓意著對於數據處理和隱私保護的平衡與透明度，強調了保密性和透明度的重要性，以確保數據處理的合規和合理性。

(III)數據分類和敏感度

E. 資料分類

1. 自身資料
自身資料是指個人所擁有的數據或信息。這些數據可以包括個人身份信息（如姓名、地址、電話號碼）、個人偏好（如喜好、興趣愛好）、個人社交媒體帳戶信息、健康記錄、金融信息、工作履歷等。自身數據是個人私有的，個人有權決定如何使用和處理這些數據。

2. 他人資料
他人資料是指與個人無直接關聯，但個人負責處理的數據。這些數據通常是他人與個人之間的關係中產生的，例如客戶的信息、僱員的信息、合作夥伴的信息等。個人在處理他人數據時，需要遵守相關的隱私法規和保密義務，確保他人數據的安全和合法使用。

F. 機密等級

1. Level 1
公開資料 - 這些是可供所有人知曉的信息，對公眾開放，沒有任何限制。例如這些信息可能是公共記錄、公告、公開發表的文件等。

2. Level 2
廣泛分享資料 - 這些是可供大部分人知曉的信息，包括廣大利害關係人。例如這些信息可能涉及組織的業務活動、產品或服務信息，可在公開場合或適當的渠道進行分享。

3. Level 3

有限分享資料 - 這些是只有少數人可以知曉的信息。例如這些信息可能包含組織的內部數據、商業機密、競爭優勢等，僅限於特定的人員或受限的利害關係人知曉。

4. Level 4
相關人/持份者資料 - 這些是可供與特定事務相關的人員或持份者知曉的信息。例如這些信息可能包括與特定項目、合同、協議或關鍵利益相關的數據。

5. Level 5
個人私密資料 - 這些是只有個人自己可以知曉的最私密的信息。這些信息可能包含個人身份信息、個人健康記錄、財務信息等，具有極高的隱私保密性。

(I) 訪問和權限控制

G. 人員權限分級

1. A級人員
A級人員屬於最高級別的人員，他們具有廣泛的訪問權限，可以訪問Level 1至Level 5的數據。他們可以自由地訪問和處理個人數據，包括公開數據、廣泛分享數據、有限分享數據、相關人/持份者數據以及個人私密數據。

2. B級人員
B級人員可以訪問Level 1至Level 4的數據。他們具有較高的訪問權限，可以訪問公開數據、廣泛分享數據、有限分享數據以及與特定事務相關的數據。然而，他們無法訪問最高級別的個人私密數據。

3. C級人員
C級人員可以訪問Level 1至Level 3的數據。他們具有較低的訪問權限，可以訪問公開數據、廣泛分享數據以及有限分享數據。他們無法訪問最高級別的個人私密數據或與特定事務相關的數據。

4. D級人員
D級人員可以訪問Level 1至Level 2的數據。他們的訪問權限較為受限，只能訪問公開數據和較低級別的數據。他們無法訪問有限分享數據、個人私密數據或與特定事務相關的數據。

5. E級人員
E級人員可以訪問Level 1的數據。他們的訪問權限最低，僅限於公開數據的訪問。他們無法訪問任何其他級別的數據，包括廣泛分享數據、有限分享數據、個人私密數據或與特定事務相關的數據。

(II) 資料處理原則

H. 自身資料的處理原則

1. Level 1
自身資料可在公開場合進行分享：這些是屬於個人的信息，可以在公開的場合自由分享，無需限制。例如，個人的姓名、職業、教育背景等可以在公開的場合自願公開。

2. Level 2
自身資料可廣泛分享，包括廣大利害關係人：這些是屬於個人的信息，可以在廣大利害關係人範圍內進行分享。這些信息可能涉及到個人的聯繫方式、工作經歷、社交媒體賬號等，可以在適當的場合與相關人員共享。

3. Level 3
自身資料僅限於少部分人知悉：這些是屬於個人的信息，僅限於很少的人知曉。這些信息可能包括個人的家庭情況、特定健康問題、個人財務信息等，只有在必要的情況下與限定的人員分享。

4. Level 4
自身資料可供與此事相關的人員或持份者知悉：這些是與特定事務相關的個人信息，可以供與該事務有關的人員或持股人知曉。例如，在特定項目、合同、協議或關鍵利益的情況下，與相關人員共享個人信息。

5. Level 5
自身資料僅供個人自己知悉：這些是個人最私密的信息，僅有個人自己可以知曉。這些信息可能包括個人的密碼、私人通信、個人日記等，只有個人自己才能具備訪問和知悉的權限。

I. 他人資料的處理原則

1. 根據數據的機密等級，遵守相應的隱私和保密規定：在處理他人數據時，需要根據數據的敏感性和機密等級，遵守相應的隱私和保密規定。這意味著需要對於高度敏感的數據採取更加嚴格的保護措施，確保數據不被未經授權的人訪問、使用或洩露。

2. 確保他人數據的安全性和隱私保護，僅在必要情況下進行分享：在處理他人數據時，應確保其安全性和隱私保護。個人數據應受到適當的技術和組織措施的保護，以防止數據的未經授權訪問、損壞或丟失。同時，在分享他人數據時，應遵循最小化原則，僅在必要情況下進行分享，並確保分享方符合適用的隱私和保密要求。

3. 尊重他人數據的所有權和隱私權，遵循法律和道德准則：在處理他人數據時，應尊重其所有權和隱私權。這意味著不得未經授權地使用、訪問或披露他人的數據。同時，還需要遵循法律和道德准則，確保在數據處理過程中遵守相關的法律法規和行業規範，尊重他人的隱私權益。

(III)制裁機制

J. 制裁機制

制裁機制是為了確保遵守《幕簾協議》的資料處理規定而設立的一系列內部制裁措施。

1. 警告函
對於輕微違規行為，首次違規者可以收到一封書面警告函，提醒其注意並遵守協議的規定。警告函的目的是起到警示作用，讓違規者意識到其行為不符合規定，並促使其改正。

2. 委託檢討
對於重復違規或較嚴重的違規行為，可以進行內部檢討委託，以確定違規行為的原因和影響。委託檢討的目的是深入瞭解違規行為的背後原因，找出問題的根源，並提出相應的改進措施。

3. 資訊培訓
對於缺乏遵守《幕簾協議》規定的知識或技能的人員，可以提供相應的資訊培訓，以加強對數據處理和隱私保護的理解和遵守能力。培訓的目的是提升人員的專業知識和技能，使其能夠更好地理解和遵守協議中的規定。

4. 內部處分
對於嚴重違反《幕簾協議》的行為，如故意洩露敏感數據或濫用他人數據，將採取相應的內部處分措施，例如停職、降職、解雇等。內部處分的目的是對違規者進行懲罰，並向組織內部傳遞一個明確的信息：嚴重違反數據處理規定將會受到嚴厲的制裁。

5. 法律追究
如果違反《幕簾協議》的行為涉及違反法律或濫用他人數據的情況，將採取相應的法律步驟，例如提起訴訟或報案。法律追究的目的是保護個人隱私權益和維護法律的權威，通過法律手段追究違規者的責任。

(IV)資料收集和使用

K. 資料收集原則

1. 合法性
數據收集必須遵守適用的隱私和數據保護法規。這包括遵守國家或地區的隱私法案、數據保護法、隱私權法以及其他適用的法律法規。確保在數據收集過程中不違反相關法律的規定。

2. 目的限制
明確定義數據收集的具體目的，並確保收集的數據僅用於實現指定的合法目的。不應超出合理範圍進行數據收集，並禁止未經授權的二次使用數據。確保數據收集的目的明確、合法且符合道德標準。

3. 資料最小化

數據收集應限於實現特定目的所需的最小範圍。採取措施確保僅收集和保留與目的相關的必要數據，並避免不必要的數據收集。最小化數據收集可以減少潛在的隱私風險和數據濫用可能性。

4. 準確性
確保收集的數據準確、完整且及時。盡量確保數據的準確性，並在必要時更新或更正數據，以維護數據的準確性和完整性。準確的數據是進行有效決策和保護個人權益的基礎。

5. 存儲期限
確定數據的存儲期限，並在超過存儲期限後根據法律和內部政策進行數據的安全銷毀或匿名化處理。合法的數據處理應該遵守規定的數據保留期限，並確保在不再需要數據時進行安全處理。

6. 獲得同意
在合法和合規的範圍內，確保取得個人的知情同意。個人在數據收集之前應該被明確告知收集的目的、數據類型、使用和分享等相關事項，並有權選擇是否同意。取得明確的同意是保護個人隱私權的重要原則。

7. 保護敏感數據
對於敏感數據（如醫療記錄、種族、宗教信仰等），應採取額外的保護措施，確保其安全性和隱私保護。敏感數據的收集和處理需要更高的安全標準和額外的防護措施，以保護個人隱私和敏感信息。

8. 跨境數據傳輸
當涉及跨境傳輸數據時，應確保符合適用的跨境數據傳輸法規，包括盡量遵循適用的隱私保護標準和機制。在跨境數據傳輸時，應注意遵守國際數據傳輸規定，並採取適當的安全措施保護數據的隱私和安全。

(V) 資料存儲和安全

L. 資料存儲和安全

1. 資料分類與標記
對收集的數據進行分類和標記，以便識別數據的敏感性和保護需求級別。例如，將數據分為機密、內部使用和公開等級。通過分類和標記數據，可以更好地瞭解數據的風險級別，並採取相應的安全措施。

2. 資料加密
對於敏感數據，應採用適當的加密技術，包括傳輸過程中的加密和數據存儲時的加密，以確保數據的保密性。加密可以防止未經授權的訪問者獲取敏感信息，並提供額外的安全保障。

3. 存取控制

實施嚴格的存取控制機制，確保只有授權人員才能訪問和處理數據。這可以包括使用身份驗證、授權機制和訪問控制清單等方式來限制對數據的訪問。存取控制有助於防止未經授權的人員獲取敏感數據，並提供數據使用的可追溯性和責任追究。

4. 防範數據洩露
建立防範數據洩露的安全措施，包括防火牆、入侵檢測系統、數據遺失防護和安全審計等。這些措施可以減少數據洩露的風險，並提供實時監測和響應異常活動的能力。

5. 防止未授權的數據修改
實施數據完整性保護措施，例如數字簽名、數據庫日誌和版本控制，以防止未經授權的數據修改。維護數據的完整性可以確保數據的準確性和可靠性，並防止惡意篡改數據。

6. 安全存儲和備份
選擇安全的存儲媒體和設施，並定期備份數據，以防止數據丟失或損毀。備份數據應存儲在安全的地點，並設置適當的訪問控制，確保數據可以進行可靠的恢復和重建。

7. 培訓和教育
提供數據存儲和安全相關的培訓和教育，確保員工具備相應的安全意識和知識，並知曉如何遵守安全措施。培訓和教育可以增強員工對數據安全的重視和合規性，降低人為失誤和安全漏洞的風險。

8. 監控和審計
建立監控和審計機制，追蹤數據存取和使用情況，及時檢測異常行為並進行相應的應對和調查。監控和審計可以幫助發現潛在的安全威脅，並提供數據訪問和使用的審計軌跡。

9. 合作夥伴管理
對於外部合作夥伴或第三方供應商，制定適當的合約條款和控制措施，確保他們遵守數據存儲和安全要求。與合作夥伴建立合適的合作關係，並明確安全責任和義務，有助於確保數據在合作過程中的安全性和保密性。

(VI)資料分享和轉移

M. 資料分享和轉移

1. 合法性
數據分享和轉移行為必須符合適用的法律、法規和合約要求。這意味著組織在進行數據分享和轉移時必須遵守隱私和數據保護法規，並確保其行為在法律範圍內是合法的。

2. 授權
在進行數據分享和轉移之前，組織必須獲得合法的授權。這包括明確獲得個人的知情同意或根據法律、法規的規定進行分享和轉移。組織需要確保授權方式符合適用法律的要求。

3. 明確目的
數據分享和轉移必須明確指定其目的。組織必須清楚地定義數據分享和轉移的目的，確保數據僅用於實現指定的合法目的，並且不超出合理範圍進行使用。數據的使用必須與事先聲明的目的一致。

4. 接收方隱私保護
在進行數據分享和轉移之前，組織必須確保接收方具備適當的隱私保護措施，能夠遵守相關的隱私和數據保護法規。組織應對接收方進行評估，以確保其具備適當的安全措施和隱私保護能力，以保護數據的安全和隱私。

5. 數據分享約定
建立明確的數據分享約定或合約對於確保合法性至關重要。這些協議應明確界定數據分享和轉移的範圍、目的、授權、保密性要求等條款，並明確雙方的責任和義務。這些協議提供了明確的指導，確保數據分享和轉移的合法性和合規性。

6. 跨境數據傳輸
當涉及跨境數據傳輸時，組織必須確保符合適用的跨境數據傳輸法規。這包括遵守適用的隱私保護標準和機制，或使用合適的法律措施（如數據轉移機制），以確保跨境傳輸的合法性和安全性。

7. 監督和審查
建立監督和審查機制是重要的步驟，用於追蹤數據分享和轉移的執行情況。組織應定期審查合作夥伴的合規性，確保其符合相關法律、法規和合約要求，並及時檢測和應對任何違規行為。

8. 數據轉移終止和追蹤
在數據分享和轉移終止時，組織必須遵守相關要求。這包括追蹤已分享的數據，並確保按照合約或法律的要求進行刪除或銷毀。組織需要採取適當的措施，確保數據在終止後不會被濫用或洩露。

(VII)個人權利保護

N. 個人權利保護

1. 透明度和知情同意
在個人信息收集和使用過程中，組織應提供充分的透明度和清晰的信息，向個人明確說明其個人信息將被用於何種目的，並獲得知情同意。這可以通過制定清晰明瞭的隱私政策和通知，以及在收集個人信息時提供必要的信息來實現。個人應當清楚知道他們的信息將如何被使用，以便做出知情的決策。

2. 最小化和目的限定
組織應僅收集和使用個人信息所需的最少量信息，並且只用於特定的合法目的，不超出事先明確的範圍。這意味著組織應避免收集不必要的個人信息，並確保所收集的信息與其所追求的特定目的密切相關。

3. 個人信息安全
為確保個人信息的安全性，組織應實施適當的技術和組織措施，防止未經授權的訪問、損毀、洩露或濫用個人信息。這可能包括使用加密技術、訪問控制、安全審計和監控等措施，以保護個人信息的機密性、完整性和可用性。

4. 存取和更正權利
個人應有權訪問其個人信息，並有權要求更正或刪除不準確、過時或不必要的信息。組織應提供適當的機制，使個人能夠行使這些權利，並在合理的時間內響應其請求。

5. 遺忘權
根據適用的法律，個人有權要求刪除與其有關的個人信息，除非存在合法的存儲或處理需求。組織應在符合法規要求的情況下，盡力滿足個人的遺忘權。

6. 可撤銷同意
個人應有權隨時撤回對其個人信息使用的同意，並要求停止進一步收集和使用個人信息。組織應建立相應的機制，允許個人方便地撤銷同意，並在收到撤銷請求後，停止使用個人信息。

7. 數據移植權
在適用的法律範圍內，個人有權要求將其個人信息轉移到其他組織或服務提供商。這可以促進個人對其個人信息的控制，並支持數據的可移植性。

8. 監管和監督機制
組織應建立獨立的監管機構或相應的監督機制，確保其遵守個人信息保護法規，並調查投訴和違規行為。這有助於確保組織按照合規要求處理個人信息，並提供一個獨立的實體監督和審查其數據處理實踐。

9. 教育和意識提升
組織應提供個人信息保護的教育和培訓，以提高個人對其權利和隱私保護的認識和意識。這可以包括培訓員工處理個人信息的最佳實踐、加強對隱私風險的認識和推廣個人信息保護的文化。

10. 法律依據和合規性
組織應確保遵守適用的個人信息保護法規和相關法律要求。這包括建立內部政策、程序和文件管理，以確保合規性，並採取適當的措施應對個人信息保護的挑戰和風險。組織應與法律和合規部門緊密合作，確保其數據保護和隱私實踐符合法律要求，並及時更新相關政策和措施以適應不斷變化的法規環境。

(VIII)資料處理監督和審查

O. 資料處理監督和審查

1. 監管機構
確定與適當的監管機構合作，根據當地的隱私和數據保護法規確保組織的數據處理活動符合相關規定。

2. 內部監控機制
建立內部監控機制，例如隱私和合規團隊，負責監督組織的數據處理實踐，確保合規性並及時檢測和應對違規行為。

3. 審查合規性
定期進行內部審查，評估組織的數據處理實踐是否符合隱私和數據保護法規，並確保相關政策和程序的有效性。

4. 隱私影響評估（PIA）
對高風險的數據處理活動進行隱私影響評估，評估可能的風險並提出相應的控制和改進措施。

5. 監控數據存取和使用
建立記錄和監控系統，追蹤數據的存取和使用情況，確保僅授予授權人員訪問個人數據。

6. 培訓和教育
提供內部培訓和教育，確保組織成員瞭解隱私和數據保護法規的要求，並掌握正確的數據處理實踐。

7. 投訴處理機制
建立有效的投訴處理機制，讓個人能夠提出與數據處理相關的投訴，並及時回應和解決投訴事項。

8. 外部審計
定期進行外部審計，由獨立的第三方機構評估組織的數據處理實踐，確保合規性並提供改進建議。

9. 文件管理和記錄保留
建立適當的文件管理和記錄保留機制，保存相關的數據處理文件和記錄，以便日後的審查和證明合規性。

10. 持續改進

根據監督和審查的結果，持續改進組織的數據處理實踐，修訂和更新相關的政策、程序和控制措施。

(IX)協議適用範圍和修訂

P. 協議適用範圍和修訂

1. 適用範圍界定
在協議中清楚地定義適用範圍，包括涵蓋的主體、範圍和地理範圍等。這有助於確定哪些實體、項目或活動受協議約束。

2. 條款明確性
協議應具備明確的條款和定義，以確保各方對協議的理解一致。這包括對關鍵術語和概念的明確定義，以避免歧義和解釋差異。

3. 修訂程序
協議應明確規定如何進行修訂。這包括指定修訂的程序、修改的提議方、審查程序以及修訂的生效條件。修訂程序應該是公平、透明和可執行的。

4. 合意原則
協議的修訂應基於各方的自願和共識。通常需要各方經過談判、協商和簽署修訂協議來達成共識。

5. 時效性和生效日期
協議應明確指定修訂的生效日期，以及修訂的有效期限。這有助於確定修訂的適用時間範圍和期限。

6. 通知機制
協議應規定對修訂的通知程序，包括如何通知各方修訂內容、生效日期和相關細節。這確保各方都能及時知曉修訂的內容。

7. 相容性
任何修訂都應與協議的其他條款相容。修訂不應違反協議的基本原則和目的。

8. 糾紛解決
協議應明確規定關於修訂的糾紛解決機制，包括進行仲裁或訴訟的程序和步驟。

9. 文件保存和版本控制
應該保存協議的各個版本，以便跟蹤修訂和確定協議的最新版本。這有助於管理和維護協議的歷史記錄，並確保使用最新的協議版本。

Q. 準據法

本協議之成立、解釋與執行應以香港法律為準據法。

1. 成立
根據該條款，本協議的成立將依據香港法律的規定。這意味著在起草、簽署和生效本協議時，各方應遵守香港法律中關於合同成立的規定。例如，符合合同要素（申請人、接受人、合法目的、合法對價等）和合同形成的要件（要約、接受、意思表示等）。

2. 解釋
當在本協議的條款解釋上存在爭議、模稜兩可或不明確之處時，將以香港法律為準據法。這意味著在解釋爭議方面，法院或爭議解決機構將參考和適用香港法律的解釋原則、法律規定和相關案例法。

3. 執行
根據該條款，本協議的執行將遵循香港法律的規定。這包括在執行本協議的過程中，各方應遵守香港法律中關於履行合同義務、違約責任和救濟措施的規定。如發生爭議，法院或爭議解決機構將依照香港法律來處理和決定相關事項。

R. 版權聲明

1. 本協議上的所有內容，包括但不限於文字、圖像、影片、音訊、腳本和其他資料，均受版權法律保護。這些內容是由版權所有者或合法授權人提供，受到國際版權法和相關法律的保護。

2. 所有內容僅供個人使用。嚴禁將本協議上的任何內容用於商業目的，包括但不限於重製、修改、散佈、傳輸、展示、表演或利用內容創建衍生作品。未經版權所有者明確書面許可，您不得以任何方式或手段使用這些內容。

3. 複製本協議內容時，您必須保留原始內容的所有版權聲明、歸屬、權利保護和其他相關資訊。禁止對內容進行修改、刪除或遮蔽任何版權聲明或其他法律聲明。

4. 轉載本協議內容時，您必須在顯著位置註明原作者姓名、原始出處及其他相關資訊，並提供鏈接到原始內容的有效鏈接。

5. 未經版權所有者明確書面許可，禁止對本協議內容進行修改、派生、散佈、銷售或任何其他形式的利用。這包括但不限於將內容用於商業目的、在其他網站或媒體上散佈內容、以及對內容進行二次創作或衍生。

6. 使用本協議內容必須遵守所有適用的法律和法規。您應負責確保您的使用符合當地法律的規定。

7. 本協議上的所有商標、標誌和圖像均為其各自所有者的財產。未經相應所有者的明確書面許可，禁止使用、複製或展示這些商標、標誌和圖像。

8. 本協議可能包含第三方內容或提供連結至其他資料。這些第三方內容或連結僅為方便用戶而提供，並不構成對這些內容的認可或評價。我們不對這些第三方內容的準確性、合法性、可靠性或完整性負責，也不承擔由此引起的任何責任。

9. 對於因使用本協議內容或存取第三方連結而產生的任何損失、損害或法律責任，我們不承擔任何責任。您自行承擔使用本網站內容的風險。

10. 本版權聲明可能隨時變更或更新，恕不另行通知。我們建議您定期檢查最新版本。

如果您對版權聲明有任何疑問，請聯絡Carson：carson.developer1125@gmail.com

S. 附則

1. 本協議未盡事宜，若需要進行變更或修訂，應經甲乙雙方書面同意或依法律規定進行。

2. 若本協議的任何條款部分無效或無法執行，不影響其他條款的效力。無效或無法執行的條款應被解釋為符合法律允許的最大範圍，並且應該盡力使協議的目的得以實現。

3. 為了證明雙方的協議，甲乙雙方在上述日期簽署了本協議的兩份副本，每方保留一份作為有效證據。

4. 本協議的任何修訂或變更應以書面形式進行，並由甲乙雙方的授權代表簽署，以確保其有效性和可執行性。

5. 本協議中的任何通知或通信，除非另有規定，應以書面形式發出，並通過註冊郵件、快遞或電子郵件等方式發送至甲乙雙方事先指定的地址或電子郵件地址。

6. 本協議的標題僅為方便起見，不應被解釋為限制或影響本協議中任何條款的含義或範圍。

7. 本協議構成甲乙雙方之間就特定事項達成的完整協議，並取代任何先前的口頭或書面協議、合同或承諾。

8. 本協議中的任何讓與、轉讓或授權應經由甲乙雙方的書面同意，除非另有規定。

9. 本協議不構成甲乙雙方之間的合夥、代理、僱傭或雇主與員工關係。甲乙雙方均為獨立的實體，並且在任何情況下都不得被視為對方的代表或代理人。

10. 本協議受到並應依據適用的法律管轄。任何與本協議相關的爭議應提交至有管轄權的法院解決。

11. 本協議的解釋、執行和履行應符合甲乙雙方所在國家/地區的相關法律法規。如有任何衝突或爭議，應以當地法院為最終解釋和裁決機構。

12. 本協議中的任何放棄權利或遲延行使權利，不構成對其他權利的放棄。任何單獨或部分行使的權利不排除對該權利的其他行使或對其他權利的行使。

13. 本協議中的任何保密條款應在協議終止後繼續有效，並繼續對甲乙雙方的保密信息和商業利益產生約束力。

14. 本協議中的任何爭議或索賠應在發生後的合理時間內提出，否則將被視為被放棄。此規定不適用於持續違反本協議的情況。

15. 本協議中的任何通知、要求或文件應以適當的方式進行交付，包括註冊郵件、快遞、電子郵件或傳真，並且應被視為在交付後即被有效提供。

16. 本協議中的任何協議或條款的廢止、修改或豁免，應經由甲乙雙方的書面同意，並且僅對該協議或條款具有約束力。

17. 本協議中的任何附圖、附件或附表均視為協議不可分割的一部分，具有相同的法律效力。

甲方	乙方
姓名:	姓名:
簽名:	簽名:
日期:	日期: