HAWKES BAY
Underwriting

資料保護政策

1. 適用範圍

本資料保護政策（「政策」）適用於Hawkes Bay Underwriting Limited（保險業監管局牌照編號：FA2078）的所有合作夥伴、員工及持牌技術代表。
本政策適用於Hawkes Bay 香港（包括Hawkes Bay Underwriting Limited）在僱傭背景下或作為提供任何產品或服務的一部分對個人資料的保護，無論是針對現任、前任或潛在的合作夥伴、員工、技術代表、保單持有人、索賠人及其他個人。
我們的所有合作夥伴、員工及持牌技術代表將收到本政策，並將通過書面通知（無論是電子發布或其他方式）不時獲悉本政策的任何重大更新、修訂或替換。每位合作夥伴、員工及持牌技術代表應遵守並受本政策約束。
如未能遵守本政策的要求，可能會導致紀律或補救行動，嚴重情況下可能終止僱傭關係。
本公司將確保其代理人、分包商、顧問及服務提供商知悉他們應遵守《個人資料（私隱）條例》（香港法例第486章）（「PDPO」）及本政策（如適用），並在處理或使用本公司持有的個人資料時實施適當的安全措施。

2. 定義

(i)「我們」、「我們的」或「本公司」在本政策中指Hawkes Bay Underwriting Limited。

(ii)「個人資料」具有PDPO（及其任何後續、替代或修訂）中定義的相同含義，即任何資料：(a) 直接或間接與一名在世個人有關；(b) 從該資料中可直接或間接確定該個人的身份；及(c) 該資料的形式使得訪問或處理該資料是可行的。

(iii)「處理」在個人資料方面具有PDPO（及其任何後續、替代或修訂）中定義的相同含義，即包括修改、增補、刪除或重新排列資料，無論是否通過自動化方式進行。

(iv)「使用」在個人資料方面具有PDPO（及其任何後續、替代或修訂）中定義的相同含義，即包括披露或轉移資料。

3. 本公司政策概述

我們非常重視個人資料的私隱保護。我們致力於按照PDPO的要求管理和保護個人資料，包括但不限於PDPO附表1中的六項資料保護原則（「DPPs」）：

(i) DPP 1：收集個人資料的目的及方式

(ii) DPP 2：個人資料的準確性及保留期限

(iii) DPP 3：個人資料的使用

(iv) DPP 4：個人資料的安全性

(v) DPP 5：資料的一般可用性

(vi) DPP 6：個人資料的訪問

除PDPO外，本公司還應遵守香港個人資料私隱專員公署（「PCPD」）發布的相關指引，特別是但不限於《保險業妥善處理客戶個人資料指引》及香港保險業監管局（「IA」）的適用要求。

本政策應與本公司的《文件創建、保存與處置政策》一併閱讀。

我們的所有合作夥伴、員工及持牌技術代表應始終尊重並妥善保管為本公司或代表本公司收集、持有、處理、存儲或使用的任何及所有個人資料的機密性。

---

4. 個人資料的收集

本公司將通過合法及公平的方式收集必要且適量（但不過量）的個人資料，用於與本公司職能、活動及服務直接相關的合法目的。

可能與本公司職能、活動及服務相關收集的個人資料的非詳盡指示性清單載於附件1。

應採取所有切實可行的步驟通知個人以下事項：

(i) 資料收集的目的及資料的使用目的；

(ii) 其個人資料可能轉移的對象類別；

(iii) 此類收集是強制性還是自願性；

(iv) 如果個人未能提供資料的後果；及

(v) 訪問及更正資料的權利。

---

5. 個人資料的準確性

本公司將採取所有合理切實可行的步驟，確保收集或保留的所有個人資料在考慮其使用目的的情況下準確無誤。

如果有合理理由相信個人資料在考慮其使用目的的情況下不準確，則不應使用該等資料。

本公司完全遵守PDPO下關於個人訪問及更正個人資料的相關義務。特別是，當個人合法要求訪問及/或更正其個人資料時，我們應按照PDPO規定的方式提供及/或更正該等資料。有關本公司訪問及更正個人資料政策的詳細信息，請參見下文第10節。

如適用，我們應驗證個人資料，包括獲取某些身份證明文件（如地址證明及個人身份證件）的副本。為確保提供給我們的身份證明文件的準確性或真實性，我們可能會根據本公司持有的現有資料進一步驗證該等資料。

---

6. 個人資料的保留

必須採取所有切實可行的步驟，確保個人資料的保留時間不超過為實現資料使用目的（包括任何直接相關目的）所需的時間。

對於不再為實現其使用目的（包括任何直接相關目的）所需的個人資料，應予以刪除（通過安全方式），除非：

(i) 任何此類刪除被法律禁止；或

(ii) 基於公共利益（包括歷史利益）不應刪除該等資料。

在此過程中，本公司不會保留個人資料超過為實現其收集目的所需的時間，除非個人資料還需保留以滿足任何適用的法律或監管要求，例如附件2中列出的要求。

我們應確保所有保留的個人資料受到與下文第8節所述相同的安全措施保護。

---

7. 個人資料的使用

本公司僅會將個人資料用於資料收集時的使用目的，除非獲得相關個人的自願及明確同意更改用途，或該等用途為PDPO所要求或允許。

本公司持有的所有個人資料將予以保密，但在必要時為滿足相關目的或直接相關目的，我們

可能會將該等資料轉移或披露給授權的第三方，或按照PDPO的要求或允許進行轉移或披露。
本公司可能會將從個人收集的個人資料轉移或以其他方式處理到該司法管轄區以外的地區。所有此類跨境資料流動應按照PDPO及該司法管轄區的資料私隱法律進行。

---

8. 個人資料的安全性

我們將個人資料的安全性視為重中之重。我們應確保個人資料免受未經授權或意外的訪問、處理或刪除。為此，本公司已實施物理、電子及管理措施和控制，以保護和保障個人資料的安全。本公司及其每位合作夥伴、員工及持牌技術代表對其持有的個人資料負責。
本公司關於個人資料安全性的政策載於附件3。

---

9. 資料的一般可用性

本公司將採取所有合理切實可行的步驟，確保個人知悉我們持有的個人資料種類、資料的主要使用目的及個人資料可能轉移的對象類別。
個人還可能有權確定本公司關於個人資料的政策和實踐，包括但不限於本政策。

---

10. 個人資料的訪問及更正

根據PDPO，個人可能有權：
(i) 確定本公司是否持有與其相關的任何個人資料，並在持有時獲取該等資料的副本；及
(ii) 要求本公司通過資料訪問請求更正其持有的不準確的個人資料，以確保其使用目的的準確性。
個人本人或其代表可行使訪問及更正權。相關人士指：
(i) 由個人書面授權提出請求的人士；
(ii) 如個人未滿18歲，其父母；
(iii) 如個人無法管理自己的事務，由法院指定管理該等事務的人士；或

(iv) 如個人精神上無行為能力，根據《精神健康條例》（第136章）指定的監護人、社會福利署署長或任何其他被授予監護權或執行指定監護人職能的人士。

個人資料訪問及更正的主要聯繫人是我們的合規官。

雖然沒有特定的表格要求，但應鼓勵個人使用PCPD網站上的《個人資料（私隱）條例——資料訪問請求表格》提交資料訪問請求，並附上適當的身份證明（例如個人身份證副本）給合規官。此服務可能會收取合理費用。資料更正請求沒有規定的表格。

在確認資料訪問請求及/或需更正的不準確之處的真實性及有效性後，本公司應在收到請求後的40天內遵守該等資料訪問請求或資料更正請求，除非本公司根據PDPO限制或拒絕該請求。

---

11. 直接促銷

除非獲得個人的明確同意且該同意未被撤回，否則本公司不得將任何個人資料用於任何直接促銷目的，或向第三方提供任何個人資料以供該等第三方用於直接促銷。

在獲得個人同意時，必須通知個人其個人資料將如何用於直接促銷。

在首次使用個人資料進行直接促銷時，應通知個人可以免費要求停止將其個人資料用於直接促銷。

---

12. 培訓與意識

本公司提供定期培訓，以確保所有合作夥伴、員工及持牌技術代表了解其在個人資料安全方面的義務。未能完成任何培訓課程可能會導致紀律或其他補救行動。

必要時應尋求合規官的建議。合規官負責提供日常協助及指導，處理資料保護相關事宜。

所有經理有責任確保其負責的領域內存在有效的控制措施，以符合本政策。高級管理層需定期確認其業務領域遵循此程序。

---

13. 資料外洩報告

資料外洩通常被視為資料使用者持有的個人資料的安全性受到懷疑的破壞，導致資料面臨未經授權或意外訪問、處理、刪除、丟失或使用的風險。它包括未經授權的第三方的訪問或其他故意行為、本公司及/或其服務提供商及/或資料處理者的故意或意外行為（或不作為）、將個人資料發送給錯誤的收件人、包含個人資料的計算設備丟失或被盜、未經許可更改個人資料，以及個人資料的可用性喪失。

資料外洩可能對個人安全、身份盜用、財務損失、羞辱或尊嚴受損、聲譽或關係受損，以及業務和就業機會的喪失構成威脅。

我們必須採取補救措施，以減輕資料外洩對資料當事人可能造成的損害或損失，同時應考慮外洩對資料當事人的可能影響。

如果懷疑或檢測到資料外洩，應立即通過電子郵件向合規官及IT官內部報告。本公司合作夥伴、員工及持牌技術代表不得向任何外部方（包括但不限於受影響的資料當事人）報告資料外洩。合規官負責此類報告，所有外部通知需經其批准。

我們在檢測到資料外洩時應採取以下行動計劃：

(i) 立即收集與外洩相關的基本信息；

(ii) 聯繫相關方並採取措施控制外洩；

(iii) 評估損害風險；

(iv) 考慮發出資料外洩通知。

上述行動計劃的詳細信息載於附件4。

合規官負責處理資料外洩事件的總體責任，包括領導初步調查並撰寫調查結果報告。

附件1

與本公司職能、活動及服務使用者相關的個人資料

- 全名
- 國籍
- 手機號碼
- 出生日期
- 身份證明文件副本
- 居住地址
- 地址證明副本
- 職業
- 銀行賬戶或信用卡資料
- 保單信息（如保單名稱及保單號碼）
- 醫療記錄
- 財務信息
- 索賠信息

與本公司員工相關的個人資料

- 全名
- 國籍
- 手機號碼
- 出生日期
- 身份證明文件副本
- 居住地址
- 地址證明副本
- 教育及專業資格
- 工作經歷
- 薪金及津貼
- 銀行賬戶資料

- 職位申請
- 評估報告
- 醫療記錄

附件2

保單持有人及索賠人

1. 根據PCPD發布的《保險業妥善處理客戶個人資料指引》，一般而言，保險機構（包括持牌保險代理機構）可保留個人資料不超過7年，自業務關係結束（例如客戶退保）之日起計算，以遵守各種法律或監管要求（如保存賬簿或客戶記錄、處理潛在訴訟等）。然而，不同類型的個人資料可能需要不同的保留期限，可能短於或長於7年，每種情況需根據其具體情況考慮。在此方面，本公司可能會不時確定某些業務記錄的保留期限應更短或更長，以符合法律或監管要求或內部決定。

2. 本公司將保留以下與客戶身份相關的文件或記錄以用於反洗錢目的：

(i) 在識別及驗證客戶及/或受益人（如適用）身份過程中獲得的任何資料及信息；

(ii) 在客戶盡職調查及持續監控過程中獲得的任何額外信息，包括簡化盡職調查或加強盡職調查；

(iii) 如適用，關於業務關係目的及性質的任何資料及信息；

(iv) 與客戶賬戶相關的任何記錄（例如開戶表格、保險申請表格或風險評估表格）及與客戶的業務往來（至少應包括與客戶盡職調查措施相關的業務往來材料或賬戶運作的重大變更）；及

(v) 任何分析結果（例如為確定複雜、金額異常或模式異常且無明顯合法目的的交易的背景及目的而進行的查詢）。

3. 所有上述反洗錢相關的客戶盡職調查文件或記錄將在與客戶的業務關係期間及業務關係結束/相關客戶賬戶關閉後5年內保留。對於包含個人資料的記錄（如個人銀行賬戶持有人的姓名），資料的保留時間不得超過必要時間。

員工

4. 未成功申請者的個人資料可保留至拒絕申請之日起2年，之後應予以銷毀。如果有持續存在的理由要求保留資料，或申請者同意將資料保留超過2年，則資料可保留更長時間。

5. 前員工的個人資料可保留至其離職之日起7年。如果有持續存在的理由要求保留資料，或資料為履行合同或法律義務所需，則資料可保留更長時間。

附件3

1. 個人資料的訪問

未經授權訪問包含個人資料的記錄及信息是嚴格禁止的。所有合作夥伴、員工及持牌技術代表無論在任何地點均負有保密義務。個人資料的訪問僅限於根據其職責「需要知悉」的合作夥伴、員工及/或持牌技術代表。

2. 物理資料

(i) 本公司已實施物理安全控制措施，包括對場所的受控訪問、視頻監控、防入侵警報及煙霧探測器，以保護個人資料免受未經授權及/或意外的訪問、處理、刪除、丟失、披露、破壞及/或損壞。

(ii) 我們實行清桌政策。包含個人資料的物理記錄在不使用時應安全存放在上鎖的櫃子中。

(iii) 所有包含個人資料的文件在使用後應進行碎紙處理並銷毀。

(iv) 應避免將紙質文件帶離辦公場所。如果必要，所有個人資料及受限信息應在文件帶離辦公場所前進行遮蓋或移除。每位合作夥伴、員工及持牌技術代表應維護一份登記冊，以記錄他們帶回家並返回辦公場所的文件。不得在辦公場所外處置包含個人資料的紙質文件。

3. 電子資料

雖然無法保證通過互聯網傳輸或電子存儲的方法100%安全，但我們將盡最大努力防止任何未經授權的訪問。
電子個人資料存儲在嚴格控制訪問的計算機系統及存儲媒體中，並進行加密，位於限制區域內及/或受到其他適當措施保護，以防止未經授權的訪問或更改。
我們的所有合作夥伴、員工及持牌技術代表將收到我們的信息安全政策，並將通過書面通知（無論是電子發布或其他方式）不時獲悉信息安全政策的任何重大更新、修訂或替換。每位合作夥伴、員工及持牌技術代表應遵守並受我們的信息安全政策約束。
以下是一些關於電子個人資料信息安全措施的相關措施及控制（詳情請參閱信息安全政

策）：

(i) 要求使用複雜密碼（包含字母、數字及/或符號的組合）以訪問任何系統。

(ii) 定期備份所有電子資料並對備份進行加密以進行異地存儲。

(iii) 所有電子資料僅可在本公司發放或批准的設備或電子設備上使用，或通過本公司運營的安全企業網站使用。特別是，所有電子及便攜設備（例如智能手機及筆記本電腦）應：

- 使用強密碼加密，並定期更改密碼；
- 使用多因素認證（如可用）；
- 定期進行系統更新；
- 安裝適當的防病毒及防惡意軟件、防火牆及最新的安全補丁；
- 啟用遠程擦除功能，以便在設備丟失時擦除其中的信息；
- 除非鎖在安全的地方，否則不得在辦公場所外無人看管；
- 避免在設備上顯眼地放置公司名稱、標誌及其他標識，以避免不必要的注意。

(iv) 僅應使用公司電子郵件賬戶發送及接收與工作相關的文件及信息，並在發送包含個人資料的文件前進行加密。

(v) 本公司提供的電子設備不得與任何第三方共享，個人設備（例如個人USB閃存驅動器）不得插入本公司提供的電子設備中。

(vi) 所有本公司提供的電子設備及IT設備必須在僱傭及/或服務合同終止時歸還。

(vii) 所有計算機系統均具有訪問控制列表，確保文件使用可在個人及角色或組級別進行控制。所有個人資料的使用均需接受審計。

(viii) 使用視頻會議軟件時，應優先選擇具有端到端加密的軟件。每次視頻會議應設置唯一的會議ID及密碼。會議ID及密碼應僅提供給預定參與者。

(ix) VPN的安全性通過以下方式確保：例如，使用多因素認證連接VPN、保持VPN平台的安全設置最新、使用握手協議在電子設備與公司網絡之間建立安全通信通道、盡可能使用全隧道VPN，以及阻止來自不安全設備的連接。

(x) 實施網絡分段以降低資料外洩事件的風險及影響，並增強對關鍵及敏感資料的保護。

(xi) 遠程訪問控制僅授予根據其職責「需要知悉」的合作夥伴、員工及/或持牌技術代表。

(xii) 遠程訪問賬戶在多次登錄失敗後將被鎖定。

(xiii) 遠程訪問日誌將被審查以識別任何可疑活動。

4. 處理者的使用

本公司對其資料處理者進行適當的盡職調查，包括評估其安全措施，並通過包含符合PDPO的資料保護條款的書面協議與其處理者合作。與其他代理人、分包商、顧問及服務提供商一樣，本公司的資料處理者知悉他們應遵守PDPO及本政策（如適用），並在處理或使用本公司持有的個人資料時實施適當的安全措施。

5. 修補政策

(i) 本公司電子設備的固件應定期及及時更新及修補，但更新及修補應僅從可信網站下載。

(ii) 本公司提供的所有電子設備運行Microsoft操作系統及Microsoft Office套件。這些設備配置為通過Microsoft更新服務自動下載並應用修補及更新。

(iii) CITRIX（我們的承保平台）由供應商 Reinfo Asia Limited託管，他們將根據合同條款修補及更新平台。本公司將確保相關合同包含符合PDPO的資料安全條款。

(iv) 防病毒及防惡意軟件檢測程序配置為每2小時檢查一次更新。

(v) 未經本公司事先明確同意，不得禁用上述自動更新及修補。

附件4

資料外洩行動計劃

1. 立即收集與外洩相關的基本信息

應迅速收集以下相關信息以評估對資料當事人的影響：

(i) 外洩何時發生？

(ii) 外洩發生在何處？

(iii) 外洩是如何被發現的，由誰發現？

(iv) 外洩的原因是什麼？

(v) 涉及哪些種類及範圍的個人資料？

(vi) 有多少資料當事人受到影響？

2. 聯繫相關方並採取措施控制外洩

檢測到外洩後，本公司應採取措施識別外洩原因並阻止外洩。合規官將在適當情況下通知人力資源官及/或高級管理層，並決定是否需要聯繫執法機構（例如警方）、相關監管機構（例如PCPD）、互聯網公司（例如Google）及/或IT專家以進行報告、建議及協助。

我們還將在適用情況下採取以下控制措施：

(i) 如果外洩由系統故障引起，停止系統運行；

(ii) 更改用戶密碼及系統配置以控制訪問及使用；

(iii) 考慮是否需要內部或外部技術援助以修復系統漏洞及/或阻止黑客攻擊；

(iv) 停止或更改涉嫌導致外洩的個人的訪問權限；

(v) 如果身份盜用或其他犯罪行為已經或可能發生，通知相關執法機構；

(vi) 保留外洩證據，以便於調查及採取糾正措施；

(vii) 如果外洩由資料處理者的行為或疏忽引起，資料處理者需向本公司及/或其他相關方報告外洩情況，立即採取補救措施，並向本公司報告進展。

3. 評估損害風險

合規官將進行風險評估，以確定資料當事人在外洩中可能遭受的損害程度，例如是否存在實際損害風險。

4. 考慮發出資料外洩通知

如果可以識別資料當事人且合規官合理預見外洩存在實際損害風險，我們將在檢測到外洩後盡快正式通知受影響的資料當事人及相關方，包括但不限於執法機構、PCPD、任何其他相關監管機構，以及能夠採取補救措施保護個人資料私隱及受影響資料當事人利益的其他方。根據案件情況，通知可能包括以下信息：

(i) 事件的一般描述；

(ii) 外洩的日期及時間，及其方向（如適用）；

(iii) 外洩的來源；

(iv) 涉及的個人資料類型列表；

(v) 對外洩可能造成的損害風險的評估；

(vi) 已採取或將採取的措施的描述，以防止進一步的損失、未經授權的訪問或個人資料洩露；

(vii) 合規官的聯繫信息，以便受影響的資料當事人獲取更多信息及協助；

(viii) 資料當事人可以採取的行動信息及建議，以保護自己免受外洩的不利影響及身份盜用或欺詐；及

(ix) 是否已通知執法機構、PCPD及其他相關方。

通知應以書面形式進行。如果無法立即識別資料當事人或存在公共利益，我們可以通過公司網站進行公開通知，前提是此方法不會增加受影響資料當事人的損害風險。

文件所有者	合規官		文件編號	COMP-HK-002
版本	**日期**	**審核人**	**更新內容**	**下次審核時間**
V1.0	22/8/2022	Joseph Lo & Elsa Wong	全面審查並更新以符合香港監管要求	2023年8月