寶雅國際股份有險公司
個人資料檔案安全維護計畫
個人資料保護管理政策

一、個人資料保護管理政策

（一）本公司為遵守、落實我國個人資料保護相關法令規定，特訂定個人資料保護管理政策。

（二）本公司應確保以合理安全之方式，於特定目的範圍內，蒐集、處理或利用個人資料；如委託他人蒐集、處理或利用個人資料時，亦應妥善監督受託者，課予受託者個人資料安全保護責任。

（三）本公司應設置聯絡窗口，供個人資料當事人行使其個人資料相關權利，或提出相關申訴、陳情與諮詢，並負責處理、協調、聯繫等相關事宜，且應規劃緊急應變程序，以防止、處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故，另應盡善良管理人之注意義務，以建立個人資料當事人信任基礎，及維護個人資料當事人權益。

（四）本公司應提供適當之安全管理措施，保護本公司所蒐集、處理或利用之個人資料檔案，並應持續維運個人資料檔案安全維護計畫，以確保個人資料檔案之安全。

二、目的與適用範圍

（一）為遵循個人資料保護法暨相關法規，防止個人資料被竊取、竄改、毀損、滅失或洩漏，本公司依本「個人資料檔案安全維護計畫」（下稱「本計畫」）辦理個人資料檔案安全維護及業務終止後個人資料處理等事項。

（二）本計畫適用於本公司業務行為所接觸之個人資料當事人（下稱「個資當事人」），包括但不限於消費者、本公司網路或實體會員、活動參與者等，及本公司內部經理人、員工、合作廠商人員等。前述適用範圍並應依經濟部等主管機關解釋調整之。

（三）本計畫應公告周知最新版本於本公司員工，使其明確瞭解及遵循。

（四）遵循法規

1. 個人資料保護法及施行細則。
2. 數位經濟相關產業個人資料檔案安全維護管理辦法。
3. 綜合商品零售業個人資料檔案安全維護管理辦法。

三、資源配置

（一）專責人員

1. 本公司應指定人員負責規劃、訂定、修正、執行本計畫，辦理個人資料檔案安全維護及業務終止後個人資料處理事項。
2. 為利本計畫之運行，本公司之專責人員為個人資料保護管理組織（下稱「本組織」）。本組織之架構，最高層級為最高管理代表，由本公司總經理擔任，並由最高管理代表領導個人資料管理委員會，定期檢視本公司個人資料保護管理制度及本計畫運作狀況。
3. 個人資料管理委員會成員原則為資訊安全部、法務室，並綜理本計畫項目之實際執行，包括但不限於制度維運、教育訓練、稽核內評等，最高管理代表並得視實際需求增加不同部門成員，以利本計畫順利推動。
4. 為輔助本組織執行本計畫，本公司各部門將指派「個人資料管理人員」1 名以配合宣達及落實本組織就本計畫公布之規範。

（二）所屬人員

凡於本公司執行業務過程中，接觸適用本計畫之個人資料之人員均為本計畫所規範之所屬人員。凡所屬人員均應遵循本計畫辦理相關事宜。

（三）查核人員

本公司應指定查核人員負責定期或不定期稽核本計畫之執行情形及成效。查核人員由各部門之個人資料管理人員擔任，並受本組織指示進行稽核，並由本組織將稽核結果向本公司提出報告。

（四）本計畫之訂定或修正，應由本組織執行之，並將訂定或修正後版本送本公司董事會核定之。

四、個人資料之範圍及項目

（一）本計畫相關之特定目的：行銷；契約或類似契約或其他法律關係事務之管理；消費者、客戶管理與服務；消費者保護；廣告或商業行為管理；分析與統計調查，及其他與本公司業務相關之事項。

（二）適用本計畫個人資料之範圍及項目：姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

五、個人資料蒐集、處理及利用之內部管理程序

（一）本公司進行個人資料之蒐集、處理或利用時，應尊重個人資料當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

（二）本公司所屬人員因業務需要而蒐集、處理、利用適用本計畫之個人資料時，應界定所蒐集、處理及利用個人資料之類別或範圍以及必要性，遵循前項要求，並應於符合本計畫第四條所定之特定目的必要範圍為之；如有疑問時，應與所屬部門個人資料管理人員討論。蒐集、處理個人資料時，應符合個人資料保護法第六條第一項或第十九條第一項所定之法定情形（至少一種）及特定目的，或有其他合法事由，且應符合個人資料保護法第七條第一項規定。

（三）本公司所屬人員直接向個資當事人蒐集適用本計畫之個人資料時，應以便利當事人的適當方式，明確告知以下事項：

1. 本公司名稱。
2. 蒐集特定目的。
3. 個人資料之類別。
4. 個人資料利用之期間、地區、對象及方式。
5. 個資當事人得請求查詢、閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料，以及行使該等權利之方式。
6. 個資當事人得自由選擇提供個人資料時，不提供將對其權

益之影響。

前述告知事項之內容及方式，所屬人員應先與所屬部門個人資料管理人員確認後為之。如有個人資料保護法第八條第二項或第九條第二項免為告知之情形，應與個人資料管理人員確認其合法依據，並通報本組織再次確認後。

（四）本公司所屬人員所蒐集適用本計畫之個人資料，非由個資當事人提供時（即「間接蒐集」），至遲應於處理或利用個人資料前，向個資當事人告知個人資料來源及前項應告知之事項，前述告知事項之內容及方式，所屬人員應先與所屬部門個人資料管理人員確認後為之。如有免為告知之情形，應與個人資料管理人員確認其合法依據，並通報本組織再次確認。

（五）本公司所屬人員利用個資時，應符合蒐集時之特定目的。如有必要進行特定目的外之利用時，應先行檢視是否符合個人資料保護法第二十條第一項但書規定，並與所屬部門個人資料管理人員確認其合法依據，再與本組織確認符合法律規定後始得為之。同時，如係依當事人書面同意而為特定目的外利用者，應確認已符合個人資料保護法第七條第二項有關書面同意之規定。

（六）本公司所屬人員於業務行為而涉及到個資有特定目的消失、期限屆滿、有個人資料保護法第十九條第二項所定情形，或有違反個人資料保護法規定而為個人資料之蒐集、處理或利用時，應依法刪除或停止蒐集、處理、利用個人資料。如於特定目的消失或期限屆滿，而未刪除、停止處理或利用個人資料時，須因執行業務所必須或經當事人書面同意。此應與個人資料管理人員確認其合法依據及作法，再與本組織確認符合法律規定後始得為之。

六、個資盤點及風險評估

（一）個資盤點：本公司所保有個資之各部門，應建立個人資料檔案清冊及個人資料作業流程說明文件。部門之個人資料管理人員應適時並每年度定期清查（預計為每年 12 月）該部門所保有之個人資料檔案，及其蒐集、處理或利用個人資料之作業流程。如發現有非屬特定目的必要範圍內之個人資料或特定目的消

失、期限屆至而無保存必要者，應予刪除、銷毀、停止蒐集、處理、利用或為其他適當之處置，並向本組織報告。

（二）個資風險評估：本公司應適時並每年定期評估（預計為每年 12 月）因蒐集、處理或利用個人資料可能面臨的法律或其他風險，並進行適當之管控及因應。

七、個資行銷行為

（一）行銷：本公司所屬人員首次利用適用本計畫之個人資料為宣傳、推廣或行銷時，應明確告知個資當事人本公司名稱及個人資料來源，提供個資當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷之方式及管道，並支付所需費用。

（二）個資當事人或其法定代理人表示拒絕接受宣傳、推廣或行銷時，所屬人員應立即停止利用其個人資料為宣傳、推廣或行銷，並將拒絕情形通報所屬部門個人資料管理人員，由部門個人資料管理人員向本組織通報，再由本組織彙整後周知本公司全體人員，並應採行防範所屬人員再次行銷之措施。

八、個資國際傳輸行為

（一）本公司就保有之個資有國際傳輸行為時，應於進行國際傳輸前，針對該次傳輸進行可能之影響及風險分析，並採取適當安全保護措施。

（二）本公司同時並應檢視是否受數位發展部或其他主管機關限制，並且告知其個人資料所欲國際傳輸之區域，同時對資料接收方為下列事項之監督：

1. 預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。
2. 當事人行使個人資料保護法第三條所定權利之相關事項。

九、個資委託相關程序

（一）本公司如委託他人蒐集、處理或利用適用本計畫之個人資料之全部或一部時，應依個人資料保護法及相關法規規定，對受託者為適當之監督，並於委託契約或相關文件中明確約定相關監督事項。

（二）本公司如受他人委託處理個人資料之全部或一部時，如認委託機關或企業之指示有違反個人資料保護法或其他個人資料保護

相關法令者，應立即通知委託機關。

十、個資當事人權利行使程序

（一）個資當事人或其法定代理人請求查詢、閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，本公司所屬人員應提供本組織或指定聯繫窗口之聯絡方式，由本組織或指定聯繫窗口依照下列方式辦理：

1. 提供行使權利之方式應考量個人資料安全管理之必要性及當事人之便利性。
2. 確認為個資當事人本人、法定代理人或經其委託之人。（應依適當之方式確認，或請求當事人或代為行使權利之人說明，其確為當事人本人或有權代為行使權利之人。）
3. 如認為有個人資料保護法第十條但書、第十一條第二項但書或第三項但書得拒絕個資當事人行使權利之事由時，應附理由通知個資當事人或其法定代理人等。
4. 應於個人資料保護法第十三條所定期限內，為准駁之決定；必要時，得予延長，但延長之期間不得逾個人資料保護法第十三條所定期限，並應將其原因以書面通知請求人。於得合法拒絕權利行使或得延長處理期限之情形，應將拒絕之理由或延長之原因，以書面通知當事人。
5. 個資當事人或其法定代理人請求查詢、閱覽個人資料或製給複製本者，應告知本公司依個人資料保護法第十四條規定得酌收必要成本費用。
6. 聯絡窗口為：

（二）當事人對於本公司所保有個人資料有不正確或正確性有爭議者，本公司應分別情形依個人資料保護法第十一條第一項、第二項及第五項之規定辦理。

（三）定期檢視個人資料蒐集之特定目的是否已消失或期限是否已屆滿；其特定目的消失或期限屆滿者，並應確保符合個人資料保護法第十一條第三項規定。

十一、教育訓練

（一）本公司應每年定期實施所屬人員之個人資料保護與管理認知宣導及教育訓練，使其明瞭個人資料保護相關法令之要求、人員

之責任範圍及各項個人資料保護相關作業程序、機制及措施之要求；對代表人、負責人或第三條所稱管理單位或適當組織之人員，另應依其於安全維護計畫所擔負之任務及角色，每年定期實施必要之教育訓練。

（二）如本公司所提供之綜合商品零售線上平台有供平台使用者零售商品時，對於平台使用者，進行適當之個人資料保護及管理之認知宣導或教育訓練。並訂定個人資料保護守則，要求平台使用者遵守。

（三）個資教育訓練事項由個人資料管理委員會之本組織負責規劃及執行。

十二、資料安全管理及人員管理

（一）本公司應考量業務性質、個人資料存取環境、個人資料傳輸之工具與方法及個人資料之種類、數量等因素，採取適當之人員、作業、設備及技術之安全管理措施。

（二）作業安全管理

1. 所屬人員之電腦、自動化機器設備或其他儲存媒介物（下合稱「儲存媒介物」）宜避免存取重要個人資料，如有業務上存取需求，應對其進行適當保護措施（例如，加密），並於使用後或業務存取目的已終了後刪除。
2. 所屬人員應避免使用私人儲存媒介物存取本公司於業務上取得之個人資料，如有必要時，應先取得其部門主管同意。
3. 建置個人資料檔案之電腦，不得直接作為消費者查詢之前端工具。
4. 所屬人員不宜使用非屬本公司之儲存媒介物，如有業務使用必要時，應先進行防毒偵測措施，始得讀取之。。
5. 個人資料儲存媒介物於廢棄或轉作其他用途前，應以適當方式銷毀或確實刪除該媒介物中所儲存之個人資料。委託他人執行前開行為時，亦應為適當之監督。
6. 蒐集、處理或利用個人資料時，如有加密或遮蔽之必要，應採取適當之加密或遮蔽機制。
7. 傳輸個人資料時，應有適當安全之防護機制。
8. 依據所保有個人資料之重要性，採取適當之備份機制，並比照

原件保護之。

（三）資料安全管理

1. 本公司應依業務需要設定所屬人員存取檔案之權限，以控管其接觸適用本計畫之個人資料，並由本組織定期確認權限內容之適當性及必要性。
2. 本公司所屬人員傳輸適用本計畫之個人資料時，應依傳輸方式採取必要保護措施，包括但不限於彌封、檔案加密或專線傳輸等方式。
3. 電子個人資料檔案使用完畢應即關閉檔案。
4. 存有個人資料之資通系統應設定合適之使用者帳號及識別密碼。如該資通系統與網路相聯者，應適隨時更新並執行防毒軟體，並定期執行惡意程式檢測。

（四）人員安全管理

1. 各部門確認蒐集、處理及利用個人資料之相關業務流程之負責人員。
2. 依據執行業務之特性、內容及需求，設定所屬人員關於個人資料蒐集、處理或利用，及接觸個人資料儲存媒介物之相關權限，定期檢視權限設定內容之必要性，並控管接觸個人資料之情形。
3. 本公司應要求所屬人員妥善保管個人資料之儲存媒介物，並於相關勞務契約列入保密條款。
4. 人員離職時，本公司應立即取消其使用者帳號、識別密碼及存取檔案之權限，並要求該人員將執行業務所持有之文件、資料、硬體裝置、儲存媒介辦理交接，不得攜離使用。

（五）技術安全管理

1. 採取適當之安全機制（包含設置防火牆等防止外部網路入侵方法），避免用以蒐集、處理或利用個人資料之電腦、相關設備或資通系統遭受無權限之存取，包括但不限於就個人資料之存取權限，設定必要之控管機制（包含異常存取資料行為之監控），並定期確認控管機制之有效性。
2. 確認蒐集、處理或利用個人資料之電腦、相關設備或資通系統具備必要之安全性，包括但不限於採取適當之安全機

制，因應惡意程式及系統漏洞所造成之威脅。

3. 進行資通系統或其他軟硬體測試時，應避免使用實際個人資料。如確有使用實際個人資料之必要時，應明確規定其使用之程序及安全管理方式。處理個人資料之資通系統如有變更必要時，應確保其安全性未降低。
4. 定期檢查使用於蒐集、處理或利用個人資料之電腦、相關設備或資通系統之使用狀況及個人資料存取之情形。

（六）本公司就本條所使用保護消費者個人資料之機制，應適時提醒消費者應用，並為適當之公告。

十三、事故之預防、通報及應變機制

（一）預防機制

本公司任何涉及到個資之業務活動，應識別及評估處理資料時個人資料檔案所面臨之風險，並採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

（二）通報及應變機制

1. 本公司所屬人員發現適用本計畫之個人資料遭竊取、竄改、毀損、滅失或洩漏等事故時，應立即向本組織及所屬部門個人資料管理人員通報，並協助本組織採取必要措施控制當事人損害、查明事故發生原因及責任歸屬，以降低、控制事故對當事人造成之損害。
2. 對於個人資料遭竊取、竄改、毀損、滅失或洩漏之個資當事人，本組織應以適當方式通知使其知悉事故發生原因、損害狀況及本公司已採取之因應及處理措施，與後續供當事人查詢之專線與其他查詢管道，並依地方主管機關所定通報作業及文件書表格式（附件 1）通報主管機關。
3. 發生重大事故時，應自發現事故時起算七十二小時內，依附表格式（附件 2），以電子郵件方式通報台南市政府及副知數位發展部及經濟部，並應視案情發展適時通報處理情形，以及將整體查處過程、結果與檢討等函報台南市政府並副知數位發展部及經濟部。
4. 前述所稱「重大事故」，指個人資料遭竊取、竄改、毀損、滅失或洩漏，單次達 5,000 筆個人資料檔案，將危及本公司

正常營運或大量當事人權益之情形。

5. 本組織應針對事故發生原因研議矯正及預防措施及機制，避免類似事故再度發生。
6. 本公司將以適時以電子郵件、簡訊、電話或其他便利當事人知悉之適當方式，通知當事人事故之發生與處理情形。

十四、設備安全管理

（一）基本措施

1. 本公司應依據作業內容及環境之不同，實施必要之安全環境管制。
2. 本公司應妥善維護並控管個人資料蒐集、處理或利用過程中所使用之實體設備。
3. 針對不同作業環境，建置必要之保護設備或技術。

（二）紙本個人資料檔案之安全保護設施及管理程序

1. 紙本個人資料檔案應存放於上鎖空間或進出管制區域中，非因業務需要，不得任意攜離、調閱、使用或複印。
2. 存放紙本個人資料檔案之空間、倉庫，應設置必要之門禁、防火裝置及防竊措施。
3. 丟棄重要之紙本個人資料檔案或文件時，應先以碎紙設備進行處理。

（三）電子個人資料檔案存放於儲存媒介物時，應採取下列措施：

1. 電腦、自動化機器設備及其他儲存媒介物應存放於上鎖空間或進出管制區域中或本身設置加密機制，設置使用者帳號及識別密碼，並依業務需要限制所屬人員存取檔案之權限。
2. 依儲存媒介物特性或使用方式，安裝防毒軟體、定期更新病毒碼並執行掃毒作業、或使用前執行掃毒作業。
3. 本公司之儲存媒介物如為所屬人員個人使用者，不宜私自交換使用，以防止個人資料遭未授權存取；如為共用者，所屬人員應於歸還前確認個人資料檔案已刪除或已維持淨空，僅保留必要之應用程式及軟體。
4. 儲存媒介物需報廢汰換或轉作其他用途時，應檢視該等設備所儲存之個人資料是否確實刪除。

十五、個資稽核機制

（一）本公司應定期（每年至少一次）或不定期稽核本計畫之執行情形及成效，查察本公司是否落實本計畫規範事項，針對實際或潛在不符合事項（不符合法令或有違法之虞者、本計畫未落實執行者）規劃矯正或預防措施，並確保相關措施之執行，並同時對於本公司個人資料安全維護之整體持續改善提出建議。執行矯正與預防措施時，應依照下列方式辦理：

1. 識別不符合事項及其原因。
2. 研議並執行矯正或預防措施。
3. 記錄及審查所採取措施之結果。

（二）前款查察情形及結果應載入稽核報告中，並向本公司負責人報告。

（三）個資稽核由本組織規劃及執行，應由各部門間互評（包括資訊安全部及法務室），並將互評結果通報予本組織，以利後續追蹤及檢討改善，個資稽核並得委由外部專業機構協助之。

十六、使用紀錄、軌跡資料及證據保存

（一）針對適用本計畫之個人資料，本公司應留存個人資料使用紀錄、自動化機器設備之軌跡資料及執行本計畫之相關文件、檔案等證據。

（二）本公司執行本計畫，除其他法令另有規定外，應留存下列紀錄或證據至少五年：

1. 個人資料之蒐集、處理或利用紀錄。
2. 自動化機器設備之軌跡資料。
3. 個人資料提供或移轉第三人之紀錄，該紀錄應包括提供或移轉之對象、依據、原因、方法、時間及地點等資訊。
4. 確認個人資料正確性及補充、更正之紀錄。
5. 當事人行使本法第三條之權利及處理過程之紀錄。
6. 個人資料或儲存個人資料媒體之刪除、停止處理、利用或銷毀之原因、方法、時間及地點等紀錄。
7. 存取個人資料系統之紀錄。
8. 資料備份及確認其有效性之紀錄。
9. 人員權限新增、變動及刪除之紀錄。

10. 因應事故發生所採取行為之紀錄。
11. 定期檢查處理個人資料之資訊系統之紀錄。
12. 認知宣導及教育訓練之紀錄。
13. 稽核及改善安全維護計畫之紀錄。
14. 其他必要紀錄或證據。

十七、業務終止後之個人資料處理方法

本公司因故終止業務或結束營業時，所保有之個人資料，應按實際情形依照下列方式處理，並留存相關紀錄至少五年：

（一）銷毀：

1. 方法：以碎紙設備絞碎或以物理方式破壞個人資料儲存媒介物之功能。
2. 時間：業務終止後相當期間內。
3. 地點：依銷毀方法決定其合適之處所。
4. 證明銷毀之方式：拍照或錄影存證。

（二）移轉：

1. 原因：如本公司屆時發生合併、分割或營業讓與之情形。
2. 對象：本公司屆時發生合併、分割或營業讓與之對象。
3. 方法：以紙本、儲存媒介物或其他傳輸方式進行傳遞。
4. 時間：移轉原因發生後相當期間內。
5. 地點：本公司或受移轉對象所在地。
6. 受移轉對象得保有該項個人資料之合法依據：應有個人資料保護法第十九條第一項規定作為依據。於移轉前，並應確認該第三人依法有權蒐集該個人資料，且移轉應採取合法且適當之方式為之。

（三）刪除、停止處理或利用個人資料：

1. 方法：以格式化刪除資料或以其他方式停止處理或利用個人資料。
2. 時間：業務終止後相當期間內。
3. 地點：依刪除、停止處理或利用個人資料之方法決定其合適之處所。

十八、個人資料安全維護之整體持續改善

本公司應依據本計畫執行狀況、技術發展、法令修正、業務或環境變

動，或其他因素，檢視本計畫之合宜性，每年檢視或修正，以期待本計畫持續維運。

版次	發行日期	文件變更說明
01	2024 年　月　日	

附件：個人資料侵害事故通報與紀錄表

附件：個人資料侵害事故通報與紀錄表

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td>業者名稱

通報機關</td><td colspan="2">通報時間:　　年　　月　　日　　時　　分
通報人：　　簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害情形</td><td>個人資料侵害之總筆數(大約）
_____筆</td></tr>
<tr><td>□一般個人資料:_____筆
□特種個人資料:_____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料外洩可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個人資料外洩後 72 小時內通報</td><td colspan="2">□是 □否，理由 ：</td></tr>
</table>