金財通商務科技服務(股)公司
資訊安全暨個人資料保護制度
資訊安全暨個人資料保護作業手冊

文件名稱：	資訊安全暨個人資料保護作業手冊
文件編號：	ISMS-01-001
機密等級：	一般資料
負責單位：	資訊安全暨個人資料保護小組
版　　本：	V2.0
發行日期：	2024 年 03 月 29 日

修訂紀錄

版次	修訂 日期	修訂 頁次	修訂者	修訂內容摘要
V0.1	2012/10/1	NA	陳柔方	· 遵循 ISO/IEC 27001:2005 標準與組織需求，制定本政策。
V1.0	2013/1/3	NA	陳柔方	· 建立基準，公佈發行。
V1.1	2020/12/30	整份文件	蕭景倫	· 根據公司營運需要、政府資訊安全法令與政策規定，調整公司資訊安全管理政策與目標。
V1.2	2021/06/30	第參章	蕭景倫	· 根據第三方稽核驗證之意見，參考 ISO 27001:2013 標準內容，修訂政策描述。
V2.0	2024/03/29	第貳章 第肆章	蕭景倫	· 遵循 ISO/IEC 27001:2022、ISO/IEC 27701:2019 標準與組織需求，變更文件名稱為「資訊安全暨隱私資料保護作業手冊」，建構手冊架構。 · 根據 ISO/IEC 27001:2022、ISO/IEC 27701:2019 標準結構，擬定手冊各章節內容，將原有資訊安全政策合併到手冊中，並增訂隱私保護政策。

壹、目的

本公司為了達到下列之營運與管理目標，訂定本政策。

一、核心業務之資訊化作業得以持續不間斷運作，維持內部制度管理之有效性，提升資訊服務品質。

二、確保所蒐集、處理與利用之所有資訊的機密性、完整性與正確性。

三、有關蒐集、處理與利用之個人資訊業務流程，符合「個人資料保護法」的要求。

貳、適用範圍

本文件係根據本公司管理之需要，並參考母公司玉山銀行資訊安全政策與要求、ISO/IEC 27001:2022、ISO/IEC 27701:2019、個人資料保護法、資訊安全管理法及政府資訊安全政策國際標準製定，以滿足 ISO/IEC 27001:2022 及 ISO/IEC 27701:2019 國際標準認證之要求。

本文件適用於本公司及公司所屬各部門規劃、實作、管理與改善資訊安全管理制度。

參、資訊安全暨個人資料保護制度之管理

一、資訊安全暨個人資料保護制度制訂

資訊安全暨個人資料保護小組應依據公司資訊安全暨個人資料保護政策與目標之要求，制訂、維護、推動、監控及改善資訊安全暨個人資料保護制度。

本公司資訊安全暨個人資料保護制度要求，係以滿足本公司資訊安全管理與個人資料保護風險之要求所訂定，資訊安全暨個人資料保護小組應遵循相關政策及作業規定，督導本公司同仁依規定實施各項作業流程要求。

二、資訊安全暨個人資料保護制度審查

本公司資訊安全暨個人資料保護制度由資訊安全暨個人資料保護委員會制定，並經總經理審核後發行實施。

三、資訊安全暨個人資料保護制度發行

資訊安全暨個人資料保護制度為本公司受控文件，發行後公司內各公司皆應遵循。受控版本得以紙本或非紙本方式發行；除各公司資安長授權同意外，不得提供本公司以外之人員使用。紙本資訊安全暨個人資料保護制度持有者調離工作職務時，需將紙資訊安全暨個人資料保護制度交還資訊安全委員會，辦理移交登記。紙本資訊安全暨個人資料保護制度持有者應妥善保管、防止丟失和損壞。資訊安全暨個人資料保護制度有任何更動時，資訊安全委員會應及時通知手冊持有者注意內容之修訂。

四、資訊安全暨個人資料保護制度修改

有關修改手冊之建議，應以書面形式向資訊安全委員會提出，並經資安長審核，總經理核准。個別或較微小變動宜採取換頁方式並於修改頁之備註欄內註記，有關文件修改應遵循「ISMS-02-003 文件管制作業程序書」及「ISMS-02-026 變更管理作業程序書」之規定辦理。

肆、組織全景

本公司主要業務即為產品開發及為客戶客製化開發資訊系統，將參考 ISO/IEC 31000 確認內部及外部可能影響 ISMS & PIMS 之因子，詳細作業程序描述於「ISMS-02-002 制度建立與維護作業程序書」。

一、瞭解組織全景

決定與本公司資訊安全暨個人資料保護制度目的有關、且影響資訊安全暨個人資料保護制度預期成果能力之外部及內部議題。

二、瞭解關注方的需求及期望

應決定以下事項，以瞭解關注方之需要及期望

(一) 與本公司資訊安全暨個人資料保護制度有關之關注各方。

(二) 這些關注方的相關要求事項

(三) 這些要求事項有哪些項目，將透過本公司的資訊安全暨個人資料保護制度執行結果進行說明。包括但不僅限於法律及法規要求事項，以及合約的要求。

三、決定資訊安全暨個人資料保護制度的範圍

本公司將依據全景分析結果將下列三項納入考量後確認資訊安全管理暨個人資料保護制度的範圍，並將其文件化記錄下來。應考量以下事項：

(一) “瞭解組織全景”中所提及的外部及內部議題。

(二) “瞭解關注方之需要及期望”中所提及要求事項。

(三) 本公司執行之活動與其它組織的活動之間的介面和依存性。

伍、領導

一、領導與承諾

本公司資安長負責資訊安全暨個人資料保護相關支援及資源之管控，即為 ISO/IEC 27001 和 ISO/IEC 27701 標準中所謂之高階管理階層（Top Management），其在資訊安全暨個人資料保護制度領導與溝通中承諾做到下面所列事項：

(一) 確保公司所發布之資訊安全暨個人資料保護政策和目標，與公司的營運策略方向一致。

(二) 宣導符合資訊安全暨個人資料保護制度要求的重要性。

(三) 調配人力與資源配合執行風險評鑑與進行風險處理。

(四) 將資訊安全暨個人資料保護制度要求與公司業務流程整合，確實要求遵循系統開發資安作業程序、變更管制作業程序、事故處理作業程序等。

(五) 參與管理審查會，指導並調整管理作為，確保資訊安全暨個人資料保護制度可達成預期的成果。

(六) 指揮與支援人力執行內、外部稽核之矯正措施，並確認改善狀況。

二、資訊安全暨個人資料保護政策

(一) 政策要求

1、 遵循母公司政策規定與內部控制制度要求，每年檢視公司資訊安全暨個人資料保護政策適切性，並根據檢視結果調整資訊安全暨個人資料保護政策。

2、 落實相關法令之遵循，包括智慧財產權保護法、個人資料保護法與外部單位簽訂之協議、契約。

3、 本公司成立資訊安全暨個人資料保護委員會，積極推動管理制度相關事項之計畫、執行、稽核與溝通協調，並積極辦理資訊安全與個人資料保護之教育訓練及宣導，以確保人員熟悉業務執行所負之安全責任。

4、 員工業務持有之資訊資產以公有公用為原則，依需求規劃進行分類分級，並進行業務需求考量之風險評估，達到有效之控管；資訊化作業依業務執行之實際需求，規劃營運持續管理，以確保資訊化作業之可用性。

5、 實體辦公環境及重要資訊設備機房均進行出入管制，以維持環境之安全。

6、 為防範電腦病毒及惡意軟體影響作業，除經合法授權之系統及應用軟體外，禁止使用其他非授權軟體。

7、 為確保管理制度之有效性，凡違反管理制度相關程序規範者，依相關規定審議懲處。

8、 持續改善資訊安全管理系統之承諾。

9、 本公司資訊安全暨個人資料保護政策應依照法令規定、契約要求與管理需要，提供往來機關與機構。

(二) 個人資料保護原則

本公司對於個人資料之蒐集、處理與利用，應符合以下個人資料保護原則，並依法令規定及公司政策，採取適當控制措施，保護個人資料，以確保個人資料之完整性、機密性及可用性，並於個人資料生命週期保護其免於受到未經授權之存取、破壞、使用、修改、揭露或損失之風險：

1、 同意及選擇：本公司蒐集個人資料(PII)前，依法取得個資擁有者(PII 當事人)個資蒐集與處理之授權，由 PII 當事人選擇如何處理其 PII，及不同意蒐集處理之意涵。

2、 目的適法性及規定：在為新目的蒐集或第一次使用資訊前，遵循適用之法律，向 PII 當事人說明蒐集個人資料之目的。

3、 蒐集限制：個人資料之蒐集，需符合適用之法律規定，且符合特定目的之必要範圍。

4、 資料最小化：個資蒐集、處理與利用，需符合最小化原則，僅限於與所處理個人資料相關的人員得存取個人資料，且需基於執行職務之所必需。

5、 利用、持有與揭露之限制：於法令允許時間內，持有個人資料，且需符合個人資料蒐集之目的。如需跨境傳輸個人資料，需知悉且符合相關國家的法令規定。

6、 準確性與品質：應確保所處理個人資料之正確、完整、最新與適度，且與蒐集之目的相關。變更個人資料前，應查證並確認個人資料之有效性與正確性。

7、 公開、透明與告知：提供 PII 當事人關於本公司處理個人資之政策、程序與實踐方法，包括處理目的、可能揭露對象、揭露個人資料檔案內容與形式，當處理個人資料之程序發生重大變更時，將以適當方式告知 PII 當事人。

8、 當事人參與及存取：提供 PII 當事人得存取及審查其個人資料之程序或方法，PII 當事人得依法令規定，行使其 PII 當事人之權力。

9、 可歸責性：各部門應指派個資管制人員及個資保護專人，使部門同仁遵循公司規定落實個人資料保護政策、程序與實踐。程序應包括訓練同仁具落實公司規定之能力，以及提供 PII 當事人抱怨與矯正程序。

10、 隱私遵循：定期實施稽核以查證和證明個人資料之蒐集、處理與利用，符合公司政策與程序規定。

三、資訊安全特定主題政策 (Topic-specific Policy)

(一) 個人資料保護政策

個人資料之蒐集、處理與利用，應符合法令與當事人同意書規定事項，及最小化原則。

(二) 移動裝置管理政策

所有界接到本公司網路和資訊系統之移動裝置，應經事前申請與審查核准，包括手機、筆記型電腦、平版電腦、或其他具有儲存和連線功能之移動式裝置，始可使用。

除非經個人資料管制人員事前書面許可，本公司人員不得使用移動裝置儲存含有個人資料任何形式之檔案。經允許儲存在移動裝置之個人資料檔案，應採取加密或設定通行碼保護防護，以降低個人資料外洩或遭不當利用之機會。

(三) 遠距工作管理政策

經由外部網路連接本公司系統之遠距工作，僅限連接中或普安全等級之資訊系統、非敏感個人資料和非機密級資料，且電腦應經設有本公司同意之保護機制。安全等級高之資訊系統、敏感個人資料和機密級資料之存取，僅限於本公司內部或 VPN 網路作業，不得經由未經加密保護之公眾網路連接存取。

(四) 存取管制政策

本公司系統與資料存取管制，包含實體與邏輯二部分。介接本公司之資訊資產設備，不得設於本公司外部無人看管或未具有保護機制之位置。具有存取本公司資訊系統或網路設施之設備，必須要具有唯一識別機制，且僅能由設備擁有者存取和個人工作相關之系統與資料，以便能夠監控設備存取軌跡和紀錄。擁有特別存取權限之使用者，應實施獨立監控作業。

(五) 加密機制與金鑰管理政策

本公司所有敏感個人資料和機密資料之傳輸、儲存到移動裝置，應加密處理。

本公司使用之金鑰，包括公鑰與私鑰，應事前評估，且經資安長核准。每年應定期審查金鑰的有效性，金鑰之管理，包括金鑰產生、發行、使用、保管與作廢，應由專人管理。

(六) 螢幕清空與桌面淨空政策

本公司同仁及合約約聘人員使用之電腦，包括伺服器、個人電腦、筆記型電腦和具有操作畫面之移動裝置，應設定電腦螢幕保護時間，電腦在無人操作且超過螢幕保護時間情況下，系統畫面應自動進入密碼保護狀態。

本公司同仁及合約約聘人員桌面，不應存放密碼及機密資料。人

員離開座位時，應將桌面整理淨空，敏感性文件及機密資料，應採取保護措施進行保護管理。

(七) 備份政策

本公司之資訊系統與系統中之資料，依其資訊資產可用性要求，區分為普中高三個級別。資訊系統與資料，應依其可用性要求進行備份和營運持續管理。

除因應恢復異常處理之所需，個人資料檔案備份應限制備份之資料存取，以確保個人資料完整性和機密性。

(八) 資料傳輸管理政策

在本公司內部系統間傳輸之資料，應在系統中設定保護機制。本公司與外部團體間的資料傳輸，應經事前申請與核准。本公司與外部團體間如為傳輸機密性資料，傳輸過程應有加密保護。

個人資料傳輸必需要為客戶合約授權範圍，且應符合相關法令法規之要求，如個人資料保護法、GDPR 等。

(九) 安全軟體開發政策

本公司所有專案都需建立軟體開發維護之資訊安全需求，且每位軟體開發專案工程師，每年應至少接受一次軟體分析、設計、開發及測試相關之資訊安全訓練。

軟體應能提供個人資料索引功能，以便能夠依據法令規定及合約規定、客戶要求對個人資料的複製、傳輸、利用等進行必要之處理。

(十) 委外廠商資訊安全管理政策

本公司應與委外廠商建立專案之資訊安全暨個人資料保護要求，並在委外廠商履行義務過程，實施必要之監控與管理，確保委外廠商提供之服務與產品，符合本公司資訊安全暨個人資料保護規

定。

四、管理目標

本公司之資訊安全管理目標為「在合於法令、法規與合約要求條件下，確保資訊資產及個人資料之機密性、完整性與可用性，提供持續可用之服務。」

為達成本公司資訊安全暨個人資料保護目標，本公司參考相關法令、政策與標準要求，建立資訊安全暨個人資料保護制度，對資訊安全暨個人資料保護制度實施範圍內之重要資訊資產採取適當保護措施，以維持資訊資產的機密性、完整性與可用性，使各項業務能順利且安全的執行，提供客戶優良服務並滿足其資訊安全管理與個人資料保護需求。

為確保本公司資訊安全暨個人資料保護制度之實施，能夠達成公司營運之需要，資訊安全暨個人資料保護小組應每年檢視與評估本公司之資訊安全暨個人資料保護目標，提出修訂建議，提請本公司資訊安全暨個人資料保護委員會審查核准。本公司之資訊安全暨個人資料保護目標包含以下各項：

(一) 業務(資訊)服務可用性目標。

(二) 個人資料之合法蒐集、處理與利用。

(三) 控制業務(資訊)服務，發生資料遭不當揭露事故之管理目標。

(四) 資料被竄改或未經授權存取事故之管理目標。

(五) 資訊安全管理與個人資料保護事故之處理。

(六) 資訊基礎設施管理目標。

(七) 資訊系統與資料備份管理目標。

(八) 帳號密碼設定管理目標。

(九) 控制安全區域經媒體揭露之資訊安全事故之管理目標。

(十) 營運持續維運計畫演練之管理目標。

(十一) 非計畫性之營運中斷時間之管理目標。

五、責任

(一) 本公司成立管理組織統籌管理制度相關事項之推動。

(二) 管理階層應積極參與及支持管理制度，並透過適當的標準和程序以實施本政策。

(三) 本公司全體人員、委外服務廠商與訪客等皆應遵守本政策。

(四) 本公司全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

(五) 任何危及資訊安全與個人資訊保護之行為，將視情節輕重追究其民事、刑事及行政責任之相關規定議處。

陸、規劃

一、風險與機會的處理行動

(一) 一般要求

本公司在規劃資訊安全暨個人資料保護制度時，應將第四章「了解關注方的需求及期望」中所提及的影響因子和「與 ISMS 及 PIMS 相關的關注方。」中提及的要求納入考量來確認需要應對的風險與機會，以：

1、 確保資訊安全暨個人資料保護制度能實現預期結果

2、 防止或減少意外的影響

3、 實作持續改善

4、 除此之外，本公司規劃確認:

5、 處理風險與機會的措施

6、 將處理措施整合與實作到資訊安全暨個人資料保護制度程序中

7、 評估這些措施的有效性

(二) 資訊安全風險評鑑

本公司由資訊安全暨個人資料保護小組訂定風險評鑑方法「ISMS-02-012 風險評鑑與管理作業程序書」，其內容應：

1、 具有資訊安全風險準則，包括：

(1) 風險接受準則

(2) 執行資訊安全風險評估的準則

2、 可識別資訊安全風險，保括：

(1) 應用資訊安全暨個人資料保護風險評估流程，來識別資訊安全暨個人資料保護範圍內的資訊喪失機密性、完整性、可用性和合法性之相關風險

(2) 識別風險擁有者

3、 分析資訊安全暨個人資料保護風險，應針對下列各項進行分析

(1) 風險發生後，可能導致的潛在影響

(2) 風險可能發生的可能性(機率)

(3) 確定風險等級

4、 評估資訊安全風險，進行下列各項：

(1) 將風險分析結果與風險準則進行比較

(2) 以分析之風險優先順序來進行風險處理

(三) 資訊安全風險處理

本公司之資訊安全暨個人資料保護風險處理流程訂定於「ISMS-02-012 風險評鑑與管理作業程序書」中，包含下列各項要求：

1、 以風險評鑑結果為依據，選擇適當的風險處理措施。

2、 確認所有選定的風險控制措施為必要的。

3、 風險處理計劃完成後，應與風險擁有者進行討論，並由風險擁有者確認風險處理計劃之適當性，及殘餘風險之可接受性。

二、資訊安全暨個人資料保護目標及達成目標之規劃

本公司之資訊安全暨個人資料保護目標於每年的管理審查會議中討論下一年度之資訊安全暨個人資料保護目標，並做成會議記錄，讓資訊安全暨個人資料保護相關人知悉，訂定次年度之資訊安全暨個人資料保護目標應將下列事項納入考量：

(一) 與資訊安全暨個人資料保護政策一致

(二) 可量測（如可行）

(三) 考慮適用的資訊安全暨個人資料保護要求以及風險評估和風險處理結果

(四) 與相關資訊安全暨個人資料保護人員溝通

(五) 適時更新，例如:組織架構變動、法令法規重大變更、公司營運領域或產品線有重大改變等時間點進行檢視，並根據檢視結果作必要之調整

三、產出適用性聲明書

資訊安全暨個人資料保護小組應根據 ISO/IEC 27001 及 ISO/IEC 27701 要求，每年審查與修資訊安全控制措施之「ISMS-01-002 適用性聲明書」，提請公司資訊安全暨個人資料保護委員會審查核准。

柒、支援

一、資源

本公司在建立、實作、維持及持續改善資訊安全暨個人資料保護制度的過程中，所需的資源由需求部門主管會整呈報資訊安全暨個人資料保護制度代表人審查，資安長核可，以便進行各式資源管理(包括人

力、時間、費用、各式軟硬體設備、教育訓練等等)。

二、能力

本公司依據「ISMS-02-007 組織訓練作業程序書」，確認：

(一) 確保人員在適當教育，訓練和經驗的基礎上能夠勝任資訊安全暨個人資料保護工作。

(二) 提供必要的資訊安全暨個人資料保護教育訓練及技術，並確保教育訓練及技術的有效性。

三、認知

人員在本公司的控制下從事其工作時必須有下列認知：

(一) 資訊安全暨個人資料保護政策

(二) 對能有效實施資訊安全暨個人資料保護制度的貢獻，包括資訊安全暨個人資料保護效能改進後的好處

(三) 不符合資訊安全暨個人資料保護制度要求的可能影響

四、溝通

本公司依據「ISMS-02-005 溝通管理作業程序書」中所規定之時機、需求、內容、負責人員進行內部及外部溝通，並在溝通完成後，確認溝通之有效性。

五、資訊文件化

(一) 一般

本公司的資訊安全暨個人資料保護制度文件化包括：

1、 ISO/IEC 27001:2022 標準中所要求的文件化資訊。

2、 ISO/IEC 27701:2019 標準中所要求的文件化資訊。

3、 所有被文件化的資訊均為資訊安全暨個人資料保護制度必要之文件。

(二) 創稿及更新

1、 本公司所有文件均依據「ISMS-02-003 文件管制作業程序書」進行：

2、 無論何時何地需要，它都是可用且適用的。

3、 確保其內容的完整性。

4、 所使用的版本都是最新的。

5、 所有文件都應依其機敏性被分類，且給予適當的保護。只有具有權限的人員才可取得受管控之文件。

6、 文件的分發、存取、使用、儲存、保存、修改及刪除的管理。

7、 為了規劃及施作本公司資訊安全暨個人資料保護制度，必要時得引用外來文件，如引用外來文件時應妥適的識別及管制。

捌、運作

一、運作的規劃和控制

本公司依據下列各項來規劃、施作及控制各項程序來建立資訊安全暨個人資料保護制度:

(一) 資訊安全暨個人資料保護要求

(二) 資訊安全暨個人資料保護目標

(三) 資訊安全暨個人資料保護風險管控措施

(四) 資訊安全暨個人資料保護風險處理計劃

本公司將訂定各種必要文件以規劃、建立、實作、監控及持續改善資訊安全暨個人資料保護制度時，並確保這些文件化之程序足以實現既定的資訊安全暨個人資料保護目標。

本公司依據「ISMS-02-026 變更管理作業程序書」，管制已規劃的變更，審查非預期變更的後果，必要時採取措施減少負面影響。

當委外處理發生時，本公司依據「ISMS-02-023 委外作業管理作業程序書」進行，確保所有的委外作業都在本公司的控制之下執行。

二、資訊風險評估作業

本公司依據「ISMS-02-012 風險評鑑與管理作業程序書」中所規定的時間或狀態來執行資訊安全暨個人資料保護風險評估，並作業程序規定留存所有必要記錄。

三、資訊安全風險處理

本公司依據「ISMS-02-012 風險評鑑與管理作業程序書」規定實作資訊安全風險處理計劃，並作業程序規定留存所有必要記錄。

玖、成效評估

一、監控、量測、分析及評估

本公司依據「ISMS-02-009 內部稽核作業程序書」進行資訊安全暨個人資料保護制度績效評估，該作業程序中應詳細說明：

(一) 哪些是需要監視和測量，包括資訊安全暨個人資料保護流程和控制措施；

(二) 監視、測量、分析和評估的方法，應確保結果有效；

(三) 什麼時候應執行監視和測量

(四) 誰應實施監視和測量

(五) 什麼時候應對監視和測量的結果進行分析和評估

二、內部稽核

本公司依據「ISMS-02-009 內部稽核作業程序書」進行內部稽核，提供資訊以確定資訊安全暨個人資料保護制度是否：

(一) 符合

1、 本公司資訊安全暨個人資料保護制度的要求

2、 ISO/IEC 27001:2022 和 ISO/IEC 27701:2019 標準的要求

(二) 有效的實施和維持

三、管理審查

本公司依據「ISMS-02-006 管理審查作業程序書」進行資訊安全暨個人資料保護制度實施與改善審查，以確保本公司資訊安全管理系統持續的適用性及有效性。

壹拾、 改善

一、不符合事項及矯正措施

當發生不符合時，本公司將依據「ISMS-02-010 矯正及預防作業程序書」針對不符合事項分析根因，進行矯正，避免不符合事項之再發生。

二、持續改善

本公司將依據「ISMS-02-010 矯正及預防作業程序書」持續改進資訊安全暨個人資料保護制度的適用性及有效性。

實施與修正

本政策經資訊安全暨個人資料保護委員會審查通過，由總經理核定後實施，修正時亦同。