個人資料保護管理政策

機密等級：一般

文件編號：PIMS -01-001

版次： 1.0.0

發行日期： 113 年 12 月 18 日

訂修廢紀錄

版次	發行日期	訂 修 廢 內 容 摘 要
1.0.0	113/12/18	配合 ISO 27701:2019 隱私資訊管理系統 建立初版

1. 目的

為遵循《個人資料保護法》、ISO/IEC 27001 及 ISO/IEC 27701 等國內外法規與標準之要求及落實個人資料之保護及管理，特訂定個人資料保護管理政策（以下簡稱本政策）。

本政策旨在建立一個完整且有效的隱私資訊管理系統（Privacy Information Management System, PIMS），確保本公司在進行公司內部處理或作為「個人可識別資訊（Personally Identifiable Information, PII）處理者」之角色時，能安全、合法且適當地處理公司內部個人資料或客戶（即 PII 控制者）所委託處理之個人資料，保護資料當事人之權益，維護客戶信任與本公司商譽。

2. 適用範圍

本政策適用所有(所有部門、全體員工、約聘僱人員、委外廠商及顧問)與個人資料之蒐集、處理與利用等作業相關之單位、人員、業務流程與系統。

3. 權責

3.1. 由資安長或其授權人核定、發布本程序。

3.2. 個人資料使用者

3.2.1. 不隨意存取、分享、處理個人資料。

3.2.2. 遵守組織隱私資訊管理系統標準與相關個人資料法規法令。

3.2.3. 發現個資外洩事故應立即依「個人資料保護緊急應變處理作業說明書」進行通報作業。

3.3. 個人資料管理者

3.3.1. 監督部門個人資料使用，確保符合管理系統規範。

4. 名詞定義

4.1. PII 當事人（PII Principal）：指個人資料所屬之自然人本人。

4.2. PII 控制者（PII Controller）：指決定 PII 處理之目的及方法的組織或個人。在本政策中，通常指本公司之客戶。

4.3. PII 處理者（PII Processor）：指依據 PII 控制者之指示，代其處理 PII 的組織或個人。本公司於 PIMS 範圍內之角色僅為 PII 處理者。

4.4. 隱私資訊管理系統(Privacy Information Management System，PIMS)

因應保護可能受 PII 處理影響之隱私的資訊安全管理系統。

4.5. 個人資料

指自然人之姓名、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。

4.6. 處理

指對 PII 進行的任何操作，包含記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

4.7. 國際傳輸

指將個人資料作跨國（境）之處理或利用。

4.8. 當事人

指個人資料之本人。

5. 作業內容

5.1. 為遵循 ISO 27701 及個人資料相關法令之規範，並達成本公司最高管理階層對個人資料保護之期許與要求，確保本公司所經手或間接持有之個人資料安全符合法規規範，故明訂個人資料管理政策如下：

落實個人資料之保護及管理，執行個人資料之蒐集、處理及利用等行為時，符合相關法令法規及 ISO 27701 之要求，避免人格權受侵害。

5.2. 政策聲明

個資有保障，隱私不煩惱。

5.3. 目標

5.3.1. 遵循客戶指示：所有 PII 處理活動皆須基於與客戶（PII 控制者）簽訂之有效合約，並遵循其指示，絕不逾越約定範圍，但客戶（PII 控制者）處理指示違反適用之法令，應告知客戶。

5.3.2. 確保處理安全：建立並維持與風險等級相應的技術與組織安全措施，保護 PII 在處理、傳輸及儲存過程中的機密性、完整性與可用性。

5.3.3. 透明化管理：確保 PII 的處理流程（包含委託次處理者）對客戶保持透明，並建立清晰的溝通與通報機制。

5.3.4. 持續改善：定期審查 PIMS 之有效性，並透過內部稽核、管理審查及矯正預防措施，持續改善個人資料保護之能力與績效。

5.4. 客戶協議之遵循

5.4.1. 公司僅在與客戶簽訂具法律效力之書面合約（如：委託處理合約）後，方能處理 PII。

5.4.2. 合約內容得明確界定雙方之權利與義務、處理的 PII 類型、處理期間、性質與目的，以及本公司應遵循之安全要求。

5.4.3. 對於客戶的任何指示，應予以記錄並遵循。若認為客戶指示有違反相關法令之虞，應立即向客戶提出疑慮並尋求澄清。

5.5. 個人資料之蒐集與處理

本公司為執行各項業務專案、內部行政作業等取得或蒐集之包括但不限於個人之姓名、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、職業等個人資料，應遵循個人資料保護法及 ISO 27701 標準採取適當的存取與管理措施，並與客戶簽署相關協議，確保不過度且符合目的、相關且適當並公平與合法地從事個人資料之蒐集與處理。

5.5.1. 僅在法律規定及公司各項業務作業內蒐集最少量的個人資料，並且不處理過多的個人資料。

5.5.2. 在公司各項業務作業的過程中僅於特定目的及個人資料類別內取得個人資料，並且只進行合於組織目的之蒐集、處理及利用。

5.5.3. 僅處理與公司各項業務作業內相關且適當的個人資料。

5.5.4. 確保客戶資料的獨立性與保密性，禁止將客戶委託處理之任何 PII 用於本公司自身的行銷、廣告或任何其他商業目的。

5.6. 個人資料之利用及國際傳輸

5.6.1. 本公司於利用個人資料時，除需依個資法之特定目的必要範圍內為之外，如需為特定目的以外之利用時，將依據個資法第二十條之規

定辦理；倘有需取得當事人同意之必要者，本公司應依法取得當事人之同意。

5.6.2. 本公司所蒐集、處理之個人資料，應遵循我國個資法及本公司個人資料管理系統之規範，且個人資料之使用為本公司營運或業務所需，方可為本公司承辦同仁利用。

5.6.3. 本公司取得之個人資料，如有進行國際傳輸之必要者，定謹遵不違反國家重大利益、不以迂迴方法向第三國傳輸或利用個人資料規避個資法之規定等原則辦理，倘國際條約或協定有特別規定、或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞者，本公司將不進行國際傳輸，以維護個人資料之安全。

5.6.4. 僅在合法及有適當保護的狀況下傳送個人資料至其他國家或地區。

5.7. 個人資料之調閱與異動

接獲個人資料調閱或異動之需求時，應依個資法及本公司所訂之程序，於合法範圍內進行當事人之個人資料查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除。

5.8. 個人資料之例外應用

5.8.1. 遵守個人資料保護相關法規，包含其他法規豁免例外應用。

5.8.2. 本公司因業務上所擁有之個人資料負有保密義務，除當事人之要求查閱或有下列情形外，應符合個資法第二十條及相關法令規定，並以正式公文查詢外，本公司不得對第三人揭露：

5.8.2.1.司法機關、監察機關或警政機關因偵查犯罪或調查證據所需者。

5.8.2.2.其他政府機關因執行公權力並有正當理由所需者。

5.8.2.3.與公眾生命安全有關之機關（構）為緊急救助所需者。

5.8.3. 本公司對個人資料之利用，除個資法第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

5.8.3.1.法律明文規定。

5.8.3.2.為增進公共利益。

5.8.3.3.為免除當事人之生命、身體、自由或財產上之危險。

5.8.3.4.為防止他人權益之重大危害。

5.8.3.5.公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

5.8.3.6.經當事人同意。

5.8.3.7.有利於當事人權益。

5.9. 個人資料之保護

5.9.1. 本公司成立資通安全暨個人資料管理委員會，明確定義相關人員之責任與義務。

5.9.2. 本公司建立與實施個人資料管理系統(PIMS)，以確認本政策之實行；全體員工及委外廠商應遵循隱私資訊管理系統(PIMS)之規範與要求，並依「資通安全暨個人資料管理組織程序書」，定期審查系統運作成效。

5.9.3. 為防止個人資料被竊取、竄改、毀損、滅失或洩漏，本公司設置資通安全暨個人資料管理委員會，統籌各項個人資料保護作業原則規劃事宜，並依相關法令規定辦理。

5.9.4. 資通安全暨個人資料管理委員會由總經理與其他資安相關業務人員組成，並記錄於【資通安全暨個人資料管理組織成員表】。其中由總經理擔任主任委員，各功能單位最高主管為委員。

5.9.5. 個人資料檔案應依「個人資料盤點作業管理程序書」進行分級分類管理，並針對接觸人員建立安全管理規範。

5.9.6. 為確保所有個人資料安全，應強化個人資料管理系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核。

5.9.7. 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務及重要性，考量其他輔助安全措施。

5.9.8. 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應釐定使 用範圍及調閱或存取權限。

5.9.9. 本公司各單位如遇有個人資料檔案發生遭人惡意破壞、毀損或作業不慎等安全事件，應進行緊急因應措施，並依本公司「個人資料保護緊急應變處理作業說明書」通報程序辦理。

5.9.10.本公司應設置個資保護聯絡窗口，受理當事人個資陳情、投訴、諮詢、個人權益及個人資料保護事項之協調聯繫等相關事宜。

5.9.11.本公司係以嚴密之措施、政策保護當事人之個人資料，包括本公司所有員工，均受有完整之「個資法」及隱私權保護之教育訓練。倘有洩露個資之情事者，將依法追究其民事、刑事及行政責任。

5.9.12.本公司之委外廠商或合作廠商與本公司業務合作時，均應簽訂【委外廠商保密切結書】，使其充分瞭解個人資料保護之重要性及洩露個資之法律責任。倘有違反保密義務之情事者，將依法追究其民事及刑事責任。

5.9.13.本公司於委託蒐集、處理及利用個資時，應妥善監督受委託單位，明定受委託單位個人資料安全保護責任及保密規定，並列入契約，要求受委託單位遵守並定期予以查核。

5.10.利害關係人之參與及期許

本公司個人資料保護及管理決議事項應納入管審會報告，涉及重大決議之會議紀錄應提報資通安全暨個人資料管理委員會及利害關係人（如企業雇主、本公司員工及其他與本公司相關人士等），如有任何回饋事項，將列入下次之討論議題。為確保本公司矯正預防措施之有效運作，應落實管理審查機制，本公司每年至少舉行一次管審會會議，並確實討論下列議題：

5.10.1.過往管理審查之議案的處理狀態。

5.10.2.資通訊安全或個資管理要求的變更，如上級機關要求、最高行政管理會議決議事項。

5.10.3.管理目標與指標量測結果。

5.10.4.內外部稽核結果。

5.10.5.個資事故與不符合項目之矯正情形。

5.10.6.風險評鑑結果及風險處理計畫執行進度。

5.10.7.持續改善之機會。

5.11.對於所取得之個人資料，應建立個人資料檔案清冊並適當維護相關內容。

5.12.對於個人資料之保護，將明確告知並設置諮詢管道，提供當事人有關個人資料將如何被使用及被誰利用的清楚資訊。

5.13.為保持個人資料正確性，依作業性質及個人資料主體之請求，予以保持最新，確保當事人權利。

5.14.個人資料保存期限，僅在合乎法律或規定或組織目的內進行。

5.15.尊重當事人權利，建立相關處理流程。

5.16.持續發展及實施個人資料保護管理工作，以確保政策得以落實。

5.17.個人資料保護政策之修正

本政策每年定期或因時勢變遷或法令修正等事由，予以適當修訂，並陳管審會審議通過後，公告實施，修正時亦同。

6. 作業說明

無

7. 使用表單

ISMS-04-002 【資通安全暨個人資料管理組織成員表】

ISMS-04-033 【委外廠商保密切結書】

8. 相關文件

8.1. 國際標準資通安全管理系統(ISO/IEC 27001：2022)。

8.2. 國際標準資通安全管理系統實務指導規範(ISO/IEC 27002：2022)

8.3. 國際標準個人資訊管理系統(ISO/IEC 27701：2022)。

8.4. ISMS-02-001 組織全景與溝通管理程序書。

8.5. ISMS-02-002 資通安全暨個人資料管理組織程序書。

8.6. PIMS-01-002 個人資料管理適用性聲明書。

8.7. PIMS-02-001 個人資料文件管理程序書。

8.8. PIMS-02-002 個人資料盤點作業管理程序書。

8.9. PIMS-02-003 個人資料風險評鑑與處理程序書。

8.10.PIMS-02-004 個人資料蒐集、處理、利用與安全管理程序書。

8.11.PIMS-02-005 個人資料當事人之權利聲明。

8.12.PIMS-02-006 個人資料檔案安全維護計畫。

8.13.PIMS-02-007 業務終止後個人資料處理方法。