個人資料保護管理政策

1. 目的

翔聆資訊有限公司（以下簡稱本公司）為規範各單位個人資料之蒐集、處理與利用，避免人格權受侵害，促進個人資料之合理利用，以符合個人資料保護法（以下簡稱個資法）及其施行細則之要求，並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）。

2. 適用範圍

本公司所有與個人資料之蒐集、處理與利用等作業相關之單位、人員、業務流程及系統。

3. 依據

3.1. 中華民國個人資料保護法。

3.2. 中華民國個人資料保護法施行細則。

3.3. 個人資料隱私權管理系統(ISO 27701:2019)。

4. 個人資料保護管理目標

4.1. 本公司應依個資法與其施行細則規定，就個人資料蒐集、處理、利用、國際傳輸及銷毀作業，採行適當安全維護措施。

4.2. 本公司應建立個人資料保護管理組織，推動及落實個人資料保護管理。

4.3. 本公司應確保個人資料之安全，免於因外在威脅或內部人員不當之管理及使用，致遭受竊取、竄改、毀損、滅失或洩漏等風險。

4.4. 本公司應定期辦理個人資料保護宣導教育訓練，提升本公司人員個人資料保護管理能力，以降低風險，並創造可信賴之個人資料保護環境。

4.5. 本公司應遵循相關法令規定與契約要求，克盡個人資料保護義務，落實個人資料管理制度（PIMS），並透過定期檢視或稽核等方式持續改善之。

4.6. 本公司應定期針對個人資料作業流程進行風險評鑑，鑑別可承受之風險等級，並針對不可接受之風險進行風險處理。

5. 個人資料保護原則

5.1. 公平及合法之處理。

5.2. 僅為了特定目的蒐集，且不進行不合於該目的之處理。

5.3. 適當、相關且不過度。

5.4. 保持正確及最新，並定期鑑識組織相關之利害關係者及其需求與期望。

5.5. 不保存超過需求之時間。

5.6. 遵循法定的個人權利，包括個人資料當事人對於其資料之存取。

5.7. 確保安全。

5.8. 不將資料傳輸到法令所不允許及沒有足夠保護之國家。

6. 政策內容

6.1. 個人資料保護管理組織

6.1.1. 本公司為有效執行個人資料保護管理各項工作，應成立個人資料保護管理組織（組織成員應包含高階主管），遵循相關法令規定，並持續有效地落實個人資料管理制度（PIMS），以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

6.1.2. 確認本公司相關人員在個人資料管理制度（PIMS）內之職責。

6.2. 隱私權政策

本公司應參照國家發展委員會訂頒之「政府網站版型與內容管理規範」附錄三「隱私權保護政策範例」規定，訂定本公司隱私權保護政策，並公告於本公司官網，使本公司網站之使用者瞭解各該網站蒐集、處理或利用個人資料之範圍及方式等資訊，以保障使用者之權益。

6.3. 個人資料之蒐集、處理及利用

6.3.1. 本公司應遵循個資法等相關法令規定，蒐集、處理或利用個人資料，包括但不限於自然人之姓名、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。

6.3.2. 本公司對個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不逾越特定目的之必要範圍，並與蒐集之目的具有正當合理之關聯。

6.3.3. 本公司對有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，除有個資法第 6 條第 1 項但書規定情形外，不得蒐集、處理或利用。

6.3.4. 本公司對個人資料之利用，除個資法第 6 條第 1 項所規定資料外，應於執行法定

職務必要範圍內為之，並與蒐集之特定目的相符；有為特定目的外利用之必要時，應依個資法第 16 條但書規定辦理。

6.3.5. 本公司依個資法第 6 條第 1 項但書第 6 款規定經當事人書面同意者，應符合個資法第 6 條第 2 項及個資法施行細則第 14 條所定之方式；依個資法第 15 條第 2 款及第 16 條但書第 7 款規定經當事人同意者，應符合個資法第 7 條及個資法施行細則第 15 條所定之方式。

6.3.6. 本公司國際傳輸個人資料時，應僅在合法且有適當安全維護措施之情形下為之，且依不違反國家重大利益、不以規避個資法或其他迂迴方式傳輸等原則辦理。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規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。

6.3.7. 當事人提出有關其個人資料之查詢、閱覽、製給複製本、補充或更正、停止蒐集、處理或利用、刪除等請求時，本公司應依個資法等相關法令規定，確實、迅速回應之。

6.4. 個人資料之保護

6.4.1. 本公司應建立個人資料管理制度 (PIMS)，並定期審查其運作，以有效落實本政策。本公司全體人員及受本公司委託蒐集、處理或利用個人資料者，應確實遵循個人資料管理制度（PIMS）之規範及要求。

6.4.2. 本公司就保有之個人資料檔案，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

6.4.3. 本公司各單位對於個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。

6.4.4. 本公司為強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立個人資料檔案稽核制度，並定期查核。

6.4.5. 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。

6.4.6. 個人資料輸入、輸出、存取、更新、更正、刪除或銷毀等處理行為，應釐定使用範圍及調閱或存取權限。必要時，考量採取權限區隔、資料加密機制或相關核准程序加以控管，並留存使用者身分，識別帳號與其行為紀錄，以供事後稽查。

6.4.7. 本公司各單位遇有個人資料檔案發生遭人惡意破壞毀損、作業不慎等危安事件，或有駭客攻擊等非法入侵情事，應進行緊急因應措施，並依本公司緊急應變通報程序辦理。

6.4.8. 本公司委託他人蒐集、處理或利用個人資料時，應對受託者為適當之監督，並請受託者簽立保密切結書，使其充分瞭解個人資料保護之重要性及洩露個人資料之法律責任。受託者有違反法令規定或保密義務之情事者，並依法追究其民事及刑事責任。

6.5. 本公司應以適當方式確認內、外部利害關係人參與個人資料管理制度（PIMS）之程度。

6.6. 本公司對於所取得之個人資料檔案，應建立個人資料檔案清冊，並適當維護相關內容。

6.7. 本公司應設置個人資料保護聯絡窗口，提供當事人有關個人資料將如何被利用及被何人所利用等資訊。

6.8. 本公司為維護個人資料之正確性，應依作業性質及當事人之請求，保持其為最新之狀態，以確保當事人權利。

6.9. 本公司應持續執行及改善個人資料保護管理工作，以確保本政策之落實。

7. 政策檢討

7.1. 本政策以每年檢討一次為原則，以反映本公司個人資料保護需求、相關法令、技術及國際標準要求等最新發展現況，並確保個人資料保護管理實務作業之時效性。

7.2. 遇有個人資料保護相關法令修正、社會經濟情勢變化或一般社會大眾對個人資料保護認知之變化等情事時，本政策應予以適當檢視及修正，以確保其適用性及有效性。

8. 施行

本政策經「IMS 推動小組」修訂及「執行秘書」審查後，送呈「資訊安全暨個人資料保護推動委員會」核可後，以書面、傳真、電子郵件或其他適當方式通知本公司所屬員工、業務往來及契約關係之廠商，以利共同遵守，修正時亦同。