中華航空資訊安全暨人工智慧政策

中華航空(以下簡稱本公司)為維護公司資訊與資訊資產之安全，防止未經授權之侵害，維持其機密性、完整性及可用性，並符合相關法規之要求，訂定本政策。

範圍

本公司各項資訊系統與資訊業務之資訊安全管理要求，均應參照本政策規範辦理。

適用對象

本公司員工及委外供應商人員均應熟悉本政策及相關管理程序內容，並落實相關資訊安全管理之要求。

資訊安全目標

一、取得國際標準驗證，持續改善本公司資訊安全管理制度，維護驗證之有效性。

二、落實資訊資產管理與資訊安全風險管理，使機密性資訊能在傳輸和儲存過程中得到保護。

三、透過資訊安全防護及控制措施，防止資訊資產遭受非經許可的竄改，以保持資訊之完整，維持網路安全。

四、藉由資訊安全事故通報、應變及演練相關機制與營運持續運作計畫，達到資訊資產營運持續可用。

五、定期實施資訊安全教育訓練，深化人員資訊安全認知，以促進個人資訊安全責任之建立。

六、新興資訊技術應納入資訊安全管理制度，依風險評估結果建立相應管理原則與控制要求，人工智慧(AI)應用之治理面向包括：

(一) 隱私與資料保護及資安防護：

確保 AI 系統處理資料符合適用之隱私及個人資料保護規範，採最小必要使用原則，並強化網路安全控管，定期安全措施執行，配合稽核審查作業，以防範未授權存取、資料濫用及資安威脅。

(二) 公平性與偏誤防範：

透過模型設計及定期監控評估機制，避免 AI 系統產生不當偏見或歧視，確保結果公平性與合理性。

(三) 人為監督與決策管控：

涉及飛航安全、旅客權益、法遵、人事、財務核准或其他重大影響之 AI 應用導入人為監督機制，保留人工介入、暫停、審核及最終裁量權。

(四) 透明度與可解釋性：

AI 應用具透明度，確保 AI 運作原則與決策邏輯具備合理說明能力。

(五) 責任歸屬與問責機制：

建立 AI 系統之責任歸屬與風險治理職責機制，資訊與資料提供單位需確保 AI 模型所用資料之準確性，以確保可追溯性與問責。

(六) 使用範圍與限制：

明確定義 AI 技術之應用範圍及限制，並禁止使用 AI 從事操控行為、利用弱勢、未授權的生物辨識監控、社會評分或其他違反適用法規及倫理之應用。

(七) AI 風險治理與倫理審查：

建立 AI 風險評估與分級管理流程，針對高風險應用導入倫理審查與核准機制，以降低潛在風險。

(八) 營運監控與模型管理：

建立 AI 模型持續監測機制，定期檢視模型效能、準確性及模型漂移，並進行必要修正與優化。

管理審查

本政策根據相關法規及資訊業務需求調整和修訂。

資訊安全管理制度

本公司依據 ISO 27001 國際標準建立資訊安全管理制度，並針對旅客航空訂位、票務、行銷營運流程及機場服務等相關資料網路與核心資訊系統進行驗證，已獲得台灣檢驗科技公司(SGS)頒發證書。

簽署人： 高星潘　　陳漢欽

董事長　　**總經理**

2026 年 7 月 18 日