



仁寶電腦工業股份有限公司 COMPAL ELECTRONICS, INC.

負責任人工智慧規範

■ 目的

人工智慧在帶給人們生活便利並提升工作效率的同時，可能也會出現偏見歧視、洩漏機密、危害資訊安全、侵害隱私與個人資料、侵害智慧財產權、發布不恰當言論等等風險。同仁在使用人工智慧時應兼顧永續發展與人類自主。

■ 適用對象及範圍

本辦法適用於公司所有開發與使用人工智慧應用的部門和員工。

公司各單位就所辦理之採購事項，應要求得標之部門、團體或個人遵循本政策與規範。

■ AI 系統管理政策

- ✓ **資料隱私與資安防護 (Privacy & Security by Design)**
安全性(security)-保護系統資安
隱私與個資保護-尊重資料隱私
- ✓ **公平包容與防範偏見 (Fairness & Bias Mitigation)**
公平且無歧視-避免潛在偏見
- ✓ **透明度與人類主導(Transparency & Human-in-the-loop)**
透明性(transparency)與可解釋性(explainability)
關鍵決策中保留人為介入審查點 (human-in-the-loop) 並允許人工干預或終止
- ✓ **權責歸屬與明確界線 (Accountability & Clear Boundaries)**
課責性(accountability) -明確責任歸屬
定義 AI 可與不可執行的清楚界線
- ✓ **環境永續與生態友善(Ecological Footprint)**
要求低生態足跡： 落實「綠色 AI」理念，要求 (自有 / 第三方) AI 資料中心 / 模型具低生態足跡



仁寶電腦工業股份有限公司

COMPAL ELECTRONICS, INC.

✓ 嚴格禁止之 AI 應用，堅守道德紅線

堅守道德紅線：不使用 / 部署包含操控性行為、弱勢剝削、社會評分或未授權生物特徵監控的 AI 系統 (即 EU AI Act 所界定之禁止系統)

■ 負責任 AI 管理與監督機制

為落實負責任 AI 政策成立跨部門「人工智慧管理辦公室」，負責相關機制之制定與管理等。該辦公室由資訊安全管理辦公室主導融合現有管理框架與制度，邀請其他相關部門共同組成，各部門在人工智慧管理辦公室裡所擔任之角色與權責，將於內部管理規則中另訂之。

■ 人工智慧之實際應用與使用風險

人工智慧實際應用

使用單位可運用人工智慧並搭配相關資通訊技術之應用範圍相當廣泛，例如 (但不限於) 下列應用場景：

- 教育訓練：可利用人工智慧來提升教育品質與職業訓練，包含但不限於：提升教育行政效率、建置多元教學資源、分析同仁學習狀況並推薦客製化輔助教學內容、分析人力市場對職場能力之需求以強化職業訓練、以及草擬教育政策之參考等。
- 智慧客服：可使用人工智慧之聊天機器人來提升對同仁的服務，包含但不限於：回答同仁的常見問題、詢問同仁需求並導引至專責單位、協助同仁查詢公司相關資訊、及協助同仁處理簡單且較為制式事務之參考。
- 政策行銷：運用人工智慧來強化政策行銷與利害關係人溝通，包含但不限於：協助分析輿情、了解同仁需求或痛點、協助依據同仁實際需求傳遞服務之訊息、及協助撰寫政策宣導與同仁溝通之說帖的參考。
- 醫療保健：利用人工智慧來提升醫療品質與公共健康，包含但不限於：提升醫務管理效能、監控流行病或傳染性疾病之爆發與散播、分析病歷資料與醫療影像、協助新藥開發與藥效預測、提升長期醫療照護之品質、以及草擬醫療政策之參考等。
- 資料分析：運用人工智慧進行資料清理、格式轉換與特徵汲取，從大量資料中挖掘有用資訊並進行分析與可視化，協助釐清問題、分析問題、進而形成決策之參考。



仁寶電腦工業股份有限公司

COMPAL ELECTRONICS, INC.

人工智慧助理：上述與其他多元的應用場景中，凡是以AI相關技術（如機器學習、自然語言處理等）為基礎所開發的軟體、線上服務、或裝置，足以作為推動業務的虛擬助手，皆可廣義稱為人工智慧助理，例如電子郵件處理、日程管理、文件自動生成等。

以上所述人工智慧應用場景僅是舉例，隨著人工智慧越來越成熟與普及，對人工智慧之運用必然不以上述場景為限。

■ 人工智慧的使用風險與限制

使用人工智慧固然可提升效能並強化決策能力與品質，惟亦可能出現處理失當甚至違法之風險，茲區分為絕對禁止事項、高度風險的使用態樣、中度風險的使用態樣、以及低度風險的使用態樣，分別說明如下：

絕對禁止事項

使用人工智慧涉及機敏性資料、個人隱私資訊、公務上應保密資料或未經公司同意公開的資料，或未符合法律規範且未經事前同意即使用人工智慧處理或利用特種個人資料，或未經人工檢視與確認即使用人工智慧直接做成影響同仁(或外部當事人)權利義務之決定者，通常屬於絕對禁止事項，例如：

A.當使用人工智慧涉及機敏性資料、公務上應保密資料或未經公司同意公開的資料時，除非使用公司自建或不對外聯網之地端機房，或相同資安防護等級之自控機房，於確認系統安全後再依機密等級分級使用，否則絕對禁止。

B.未符合法律規範且未經當事人之事前同意使用人工智慧對當事人進行人臉、指紋或其他生物特徵之辨識。

C.未符合法律規範且未經當事人之事前同意，使用人工智慧之輸入內容包含當事人之病歷、醫療、基因、性生活、健康檢查或犯罪前科等特種個人資料。

D.未經人工檢視與確認，使用人工智慧直接做成影響當事人權利義務之行政或法律處分。



仁寶電腦工業股份有限公司

COMPAL ELECTRONICS, INC.

E.未經人工檢視與確認，使用人工智慧直接對當事人進行評分或評核。

■ 負責任人工智慧之開發與應用管理

人工智慧開發專案之風險負責主管需對 AI 系統應用擬定 AI 目標與範圍邊界。

根據目標邀請資訊科技、法律與倫理等跨部門專業合作以下事項：

識別“起始(initial)→設計與開發→驗證與確認→部署→運作與監督→重新評估→退役”人工智慧生命週期之風險並進行衝擊分析與限制，風險衝擊分析包含機密性、完整性與可用性，亦需考量個人、群體與社會層面(含永續)影響。風險評鑑結果預先採取相應措施並以確保人工智慧的使用符合公司需求及其價值。

人工智慧應用時皆應承擔以下管理責任：

(一) 課責性：AI 系統的使用者必須為其所生成之內容負責，包含確保其內容符合事實、且遵循法律與倫理規範。鑑於當今人工智慧所生成之內容仍常出現「幻覺」與不可接受之錯誤，因此使用人工智慧協助生成文字、圖案或影片時，務必檢視並確認其正確性。

仁寶電腦「人工智慧管理辦公室」遵循 ISO27001 並參酌 ISO 42001 AI 管理系統標準，負責 AI 的結果、風險決策與法規遵循，透過建立調查與處理 AI 錯誤或造成損害的機制與可審計的資料與模型，釐清開發者、使用者與管理層的責任歸屬。

(二) 安全性：依據公司資訊資產評鑑之資通安全責任等級要求，考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全控制與維護。以確保資料、系統、設備、網路安全及人員安全，降低因人為疏失、蓄意或天然災害等導致之資通訊資產遭竊、不當使用、洩漏、竄改或破壞等風險。使用 AI 系統時應慎選平台與工具並詳細閱讀使用條款，確保符合機密分類規範，以免洩漏公司或客戶機密。使用外部或公用 AI 系統時，必須假設輸入及產出之內容皆可能被外部機構所記錄。除非透過公司自建或不對外聯網，否則不得使用 AI 系統來提問或生成機敏性文書。

(三) 透明性與可解釋性：

透明性:AI 系統應具備適當之透明性，並適當揭露其使用方式、能力、限制、資料來源及相關風險。



仁寶電腦工業股份有限公司

COMPAL ELECTRONICS, INC.

具體來說，使用者應當包含但不限於以下透明性：1. 被告知其正在與人工智慧互動；2. 提供其資料將如何被 AI 系統處理的相關資訊；3. 被告知其與 AI 系統互動過程中可做出的任何選擇；4. 知悉其擁有對人工智慧生成結果提出質疑或申訴的權利。

人工智慧系統於其生命週期中應設有可追溯性 (traceability) 措施，亦應設有持續評估輸入至人工智慧系統之資料品質與來源的措施。能產出 AI 系統決策的資料集與流程 (包括資料蒐集、資料標註，以及任何使用的演算法)，以利追溯與透明。

可解釋性：可解釋的 AI 系統採用流程與方法，讓使用者能理解的方式辨識 AI 系統採取行動背後的事實依據與推論過程。在最大可行範圍內，公司建立的 AI 系統將以能夠解釋系統決策或結果的方式進行設計、實作與使用，並能明確解釋其提問過程與所生成結果之關連。

(四) 公平且無歧視：避免在使用及 / 或開發人工智慧時產生潛在偏見，使用 AI 系統生成文字、圖案或影片時必須確保所生成之內容，對任何族群、種族、性別及社經地位均公平且無歧視。人工智慧模型的訓練樣本可能有取樣偏差而無法代表母體，或訓練時人工標註過程可能有偏見，使得 AI 系統所生成之內容帶有偏見歧視，因此對於其所生成內容務必經由人工檢視並於必要時進行修改與確認。

(五) 資料隱私與個資保護：開發 AI 系統過程必須遵守本公司[\[仁寶集團個人資料暨隱私保護政策與規範\]](#)，且必須確保 AI 系統使用的個人或機敏資料採資料最小化原則並為匿名或去識別化。對於輸入人工智慧的內容，以及對於 AI 系統所生成之內容，均應確保不包含資料隱私與個人資料，如包含員工之個人資料應以去識別化準則先進行去識別化處理。

(六) 決策中保留人為介入：應確保 AI 系統於其整體生命週期各階段，均建立適當之人為監督及介入機制，以維持其運作之可控性與監督性。

人工智慧系統之輸出結果，應納入人工審查及必要之介入程序，以確保其有效性及合理性，並具備辨識及修正潛在偏誤、錯誤或非預期結果之機制。



仁寶電腦工業股份有限公司

COMPAL ELECTRONICS, INC.

重大性、高風險或不可逆之決策事項，應納入適當之人為審核及核准程序，並於人類判斷基礎上，審慎參考人工智慧系統之輸出結果作為輔助依據，不得於無人為監督之情況下逕行決定。

(七) 環境與道德影響：

環境：建置時考量 AI 系統對環境所造成的影響。評估 AI 系統在永續性、資源保育與生態穩定等面向的相關考量。應於合理可行範圍內，確保自有或委外之人工智慧相關運算資源（如資料中心或模型）採行降低環境足跡之措施。

道德：在 AI 系統的整個生命週期中納入政府與社會道德誠信、人權以及法治等價值的考量。不使用 / 部署包含操控性行為、弱勢剝削、社會評分或未授權生物特徵監控的 AI 系統，禁止使用下列類型的 AI 系統，包含但不限於：

- (a) 部署潛意識影響或操縱性技術；
- (b) 利用個人脆弱性（例如因年齡、身心狀況或其他因素而更易受影響的情況）；
- (c) 依據個人的社會行為、社經地位，或種族 / 族裔等敏感個人資訊，以歧視性方式對人進行分類；
- (d) 使用或訓練於從社群媒體或公開可得資訊中不加區別（無差別）蒐集的生物識別資料；
- (e) 涉及蒐集敏感個人資料以進行對個人的剖析（profiling）或建立個人側寫。

透過採取負責任的人工智慧作法，努力降低環境與社會風險，並走在永續創新的最前沿。

(八) 教育訓練與善用：AI 系統之使用者皆應學習辨識其使用風險與限制，並學習如何運用其優勢以提升工作品質與效率，包含如何對人工智慧下達貼切的提詞以強化對 AI 系統的使用。仁寶亦定期針對所有人員皆進行隱私權保護之訓練，並評估訓練之有效性。

■ 零容忍政策

仁寶對於 AI 系統管理採取零容忍政策，任何人員如有違反，將依仁寶內部人事管理規章、員工獎懲規範進行相關懲處，並視情節輕重依法送辦。



仁寶電腦工業股份有限公司

COMPAL ELECTRONICS, INC.

■ 申訴與舉報

如有發生可能導致個人權益受損(包含 AI 系統之隱私防護、AI 系統公平性與偏見防範)的事件或情況，以及發現可能有違反本規範之情事，仁寶之員工、外部單位或自然人，皆可透過隱私權保護專線 +886287978588#14385，或電子郵件信箱 Compal_PIR@compal.com，進行申訴或舉報，我們將嚴格保護舉報人之相關資訊，以維護舉報人之權益。

- 本規範之變更我們將不定期修改本規範，以落實負責任人工智慧治理。當我們完成相關條款修改時，會立即將其刊登於仁寶網站，您得不定期查閱我們的人工智慧管理政策與規範，以適時更新相關必要資訊。

■ 附則

第 1 條 本規範經董事會通過後實施，修訂時亦同。

第 2 條 本規範訂定於中華民國 115 年 8 月 13 日經董事會決議通過後實施。