冠德集團使用生成式人工智慧(AI)管理辦法

一、 目的

冠德集團(含冠德建設股份有限公司暨轄下子公司、關係企業、基金會，以下簡稱本集團、公司)為強化集團成員利用生成式人工智慧(以下簡稱生成式 AI)協助執行業務或提供服務，以提升行政效率，並避免使用生成式 AI 可能帶來之資訊安全、隱私、秘密、人權、倫理及法律等風險，以符合公司資通安全政策及政府相關法規要求，特訂定本管理辦法，作為集團成員使用生成式 AI 執行業務應遵循之規範與相關道德準則。

二、 定義

（一）本辦法所稱人工智慧，係指透過大量資料學習，利用機器學習或相關建立模型之演算法，進行感知、預測、決策、規劃、推理、溝通等模仿人類學習、思考及反應模式之系統。

（二）本辦法所稱生成式人工智慧，指可以生成模擬人類智慧創造之內容的相關 AI 系統，其內容形式包括但不限於文章、圖像、音訊、影片及程式碼等。

三、 適用範圍

（一）本辦法適用於本集團所有董事、經理人、受僱人、受任人、承包商及任何獲得公司批准或提供生成式 AI 服務的第三人（以下簡稱使用人）。

（二）使用人於執行公司業務、運營、提供客戶服務等場合運用生成式 AI(包含公司內部自行開發的 AI 工具以及第三方 AI 工具)者，適用本辦法。

四、使用規範

（一）使用人應選擇符合本辦法所規定之道德標準和法令規定的第三方 AI 工具。如為公司提供的生成式 AI 工具或帳戶，應由經公司同意之部門或成員使用，且僅限使用於執行公司業務、運營、提供客戶服務等職務相關用途。

（二）生成式 AI 產出之資訊，須由業務承辦人就其風險進行客觀且專業之最終判斷，不得取代業務承辦人之自主思維、創造力及人際互動。

（三）使用人不可完全信任生成式 AI 產出之資訊，亦不得以未經確認之產出內容直接作成業務行為或作為業務決策之唯一依據。

（四）運用人工智慧技術作為對外執行業務或提供服務之輔助工具時，應適當告知該互動或服務係利用人工智慧技術自動完成，並提醒業務或服務對象得選擇是否使用。

冠德集團使用生成式人工智慧(AI)管理辦法

五、隱私與資訊安全

(一)資料隱私與機密性

1、 使用生成式AI時應確實遵循內外部有關資通安全政策、個人資料保護、營業秘密法、智慧財產權、「一般資料保護規則」(General Data Protection Regulation,GDPR)、「消費者隱私保護法」(The California Consumer Privacy Act,CCPA)、「健康保險可攜性與責任法案(HIPAA)」等相關法令規範與相關資訊使用規定，處理、儲存、傳輸與使用資料的過程中，應注意保護所有相關個人和公司的資料隱私權,具備適當的保護措施確保其系統和資料的安全,避免資料洩露，並使用相關安全技術防止、偵測和回應各種安全威脅和攻擊，如駭客攻擊、惡意軟體等。

2、 使用人不得披露、共享或輸入機密資料【包括但不限於員工或客戶的個人識別信息(Personally Identifiable Information ,PII)、設計圖、施工計畫、成本估算、投標文件、財務資訊、未經公司同意公開之資料及其他機敏資訊】，亦不得向生成式AI詢問可能涉及機密資訊、業務秘密或個人資料之問題。

3、 AI 生成的行銷分析應符合歐盟「一般資料保護規則」(General Data Protection Regulation,GDPR)、「消費者隱私保護法」(The California Consumer Privacy Act,CCPA)、個人資料保護法及公司的客戶隱私政策，且不得收集未經授權的個資。

(二)安全機制

公司應實施適當的訪問控制、加密技術及其他安全措施，以防止未經授權訪問生成式AI 工具，並應遵守相關資訊安全政策及規章，以保護公司不受網路攻擊及資安漏洞威脅。

六、人工智慧技術

(一) 公司自行開發、優化人工智慧技術時，應保存必要技術文件及相關紀錄，包括開發者在設計、開發和實施過程中，如為可能影響決策的重要資料、模型或演算法等紀錄，以確保其在必要時可被查驗。

(二)公司使用第三方人工智慧技術時應執行調查、評估及監督作業，以確保第三方業者在人工智慧運算有自行留存軌跡紀錄，俾利後續查驗。

(三)公司運用人工智慧技術的模型訓練階段中(包括進行預訓練、優化訓練等)，在選擇模型或演算法等相關工具時，應注意其安全性，並採取有效措施，包含但不限於資料品質處理、模型驗證與監控等，以提高訓練品質防止生成不適當資訊，提升人工

智慧技術的輸出或生成內容的準確性與可靠性。

七、法令遵循與道德規範

(一)使用生成式 AI 應遵守資通安全、個人資料保護、營業秘密、著作權與相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。

(二)生成式 AI 輸入與輸出內容應定期檢視，提供演算法偏見培訓，確保公平性並防止歧視，必要時得與 AI 供應商合作，以減少偏見並促進包容性。

(三)使用生成式AI 應符合公司誠信經營、倫理標準與價值觀，確保透明度與責任。

八、教育與培訓

集團成員須接受生成式AI 技術操作及法遵、道德規範相關之訓練。

九、監測與稽核

(一)公司應定期進行風險評估與績效衡量，以識別漏洞、評估 AI 效能，並解決技術應用與外部環境變化所生風險與機會，並且根據評估結果調整和改進相關的策略和措施。

(二)集團成員如發現任何疑似違反AI 使用的倫理道德、法令或其他違法本辦法之情事，應即時通報公司資訊部門。

(三)針對經授權使用之 AI 帳戶，如發現違反本辦法或使用率極低或閒置，資訊處有權得撤銷該帳戶之存取權限。

十、審查與修訂

(一)本辦法由資訊處擬訂後，經呈核總經理核准後公布施行，修訂時亦同。

(二)資訊處將根據技術發展、公司業務需求或法規變更，定期審查與更新。

(三)本辦法制定於民國 114 年 3 月 27 日。