中央警察大學人工智慧應用內控管理要點

中華民國 115 年 11 月 13 校電字第 1150010370 號函訂定發布

一、中央警察大學(以下簡稱本大學)為確保運用人工智慧執行業務、教學研究或提供服務時，能有效管理潛在風險並保障人員與民眾基本權利，落實人工智慧基本法第十九條規定，特訂定本要點。

二、本要點適用於本大學自行或委外建置、開發、採購之各類人工智慧系統與服務。

三、本大學使用人工智慧執行業務、教學研究或提供服務時，其風險管理、內部控制監督與內部控制措施辦理事項，由本大學資通安全暨個人資料保護管理會統籌辦理。

四、本大學自行開發、委外建置或採購各類人工智慧系統與服務，應遵循人工智慧基本法第四條所定之原則。

五、人工智慧系統與服務之資通安全防護，應依本大學資通安全維護計畫與資通安全管理法及其相關法令辦理；涉及個人資料蒐集、處理或利用時，應依本大學個人資料保護管理要點及個人資料保護法進行事前評估與控管。

六、本大學各單位於規劃自行開發、委外建置或採購人工智慧系統與服務前，或既有人工智慧系統與服務發生重大功能變更時，應填具政府人工智慧應用風險評估檢核表(如附表)，識別潛在風險。

七、人工智慧系統與服務經依政府人工智慧應用風險評估檢核表(如附表)規定綜合判定結果為甲類者，應辦理下列內部控制措施：

（一）人類監督保留：不得將具法律效果或影響當事人權益之行政處分與決策，完全交由人工智慧自動裁定，應保留適當之人為介入與最終覆核機制。

（二）透明標示：系統與服務自動生成之圖文內容或提供對外互動服務(如客服機器人、校務諮詢系統)時，應於顯著處標示「本內容由人工智慧輔助/生成」等提示。

（三）明確警語：應明確標示注意事項或警語。

（四）建立救濟機制：針對受人工智慧輔助決策影響權益之當事人，應提供明確之申訴管道、決策解釋及權益救濟流程。

（五）強化防護：應於採購契約或系統與服務規格中，加重對供應商之資安、資料治理與防範歧視偏見之要求。

八、人工智慧系統與服務經依政府人工智慧應用風險評估檢核表(如附表)

規定綜合判定結果為乙類者，應辦理前點所列各款內部控制措施，並依本大學資源，優先處理甲類風險部分。

九、人工智慧系統與服務經依政府人工智慧應用風險評估檢核表(如附表)規定綜合判定結果為丙類者，應辦理第七點第一款及第二款內部控制措施。

十、人工智慧系統與服務於運行中，若發生第七點綜合判定結果為甲類、演算法嚴重偏差、生成重大違法內容、資料外洩或對當事人權益產生實質損害等異常情事，業務單位應立即暫停系統與服務部分或全部功能、啟動人工備援作業或其他因應措施，並依本大學資通安全事件通報及應變管理程序書進行通報；如為資通安全事件外之異常情事，依內部控制或相關機制處理。

十一、本大學應定期辦理並鼓勵教職員生參與人工智慧素養、資訊倫理及風險管理之教育訓練，使其瞭解人工智慧之應用，應避免有侵害人民生命、身體、自由或財產，破壞社會秩序、國家安全或生態環境，或偏差、歧視、廣告不實、資訊誤導或造假等違反相關法規之情事，以提升人員對人工智慧技術局限性及資安風險之認知。

十二、本管理要點所定內部控制機制應由本大學每年檢視，並因應技術發展及法令異動而適時做滾動式檢討。