11月份公務機密維護宣導　AI軟體與服務可能產生之風險疑慮

近年來AI軟體與服務快速發展，影響遍及全球產官學研各界。自ChatGPT於2022年底發布後，更掀起全球熱潮，且被視為人工智慧之一項重大突破。運用生成式AI軟體與服務協助執行業務或提供服務，有助於提升工作效率與創意發想。

AI軟體與服務常透過蒐集使用者輸入內容或擷取網頁文字做為訓練資料，以逐步改善模型並產出更正確之結果，故可能涉及隱私洩露之風險。另外，AI軟體與服務透過大量蒐集與訓練所產出之結果，可能涉及侵害智慧財產權、人權或商業機密之風險，且受限於訓練資料之品質與數量，可能會生成真偽難辨或創造不存在之資訊，建議針對生成結果需進行評估後再行運用。

使用AI軟體與服務時，應避免暴露個人資料與機敏資訊，同時注意內部保密義務與智慧財產權相關規定，秉持負責任及可信賴之態度，掌握自主權與控制權，並堅守安全性、隱私性與資料治理、問責等原則，不得恣意揭露未經公開之公務資訊、不得分享個人隱私資訊及不可完全信任生成資訊。

此外，有鑑於過往曾發生軟體與APP被發現重大資安疑慮情事，近期AI軟體與服務如雨後春筍般誕生之際，亦難免出現相似資安疑慮，因此選用AI軟體與服務時，需留意提供該軟體與服務之公司背景，不應盲目信任使用。

隨著針對不同使用情境不斷推陳出新之AI軟體與服務，建議企業與民眾使用前審慎評估軟體是否安全，輸入之資料是否敏感，並了解軟體開發商之隱私權政策及如何處理資安漏洞等問題，以免發生違法、洩漏敏感資訊、侵害智慧財產權及財物損失之憾事。若欲於工作中採用AI軟體與服務，可參考「行政院及所屬機關（構）使用生成式AI參考指引」，以降低可能帶來之危害與風險。

轉載自臺中市政府水利局政風室