114年6月公務機密宣導-

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。

【資料來源：台中市政府政風處】

114年6月機關安全維護宣導-

如何維護機關設施及同仁之人身安全？

一、 注意可疑之人、事、物

多數行政機關為開放式服務機關，民眾 進出洽公頻繁，要實施門禁管制實屬不易，惟可請服務臺或保全人員加強辨識可疑人物（例如：疑似攜帶危險物品、特別注意攝影機位置、穿著不合時宜、詢問特定人員位置、嘗試進入非洽公區或其他形跡詭異行為），並適時詢問洽公事由，藉由交談過程中初步判別是否有不良意圖。

二、 充實監視設備系統

在發生糾紛時，往往各說各話，惟有證據能還原事實，監視設備除了監看洽公民眾有無異常舉動以作為預警資料外，更是發生糾紛時重要的佐證資料，過去有案例於法院審理時，即因調閱監視錄影畫面，發現民眾確實有對承辦人員狀似怒罵舉動，再輔以在場人員作證怒罵內容後，使法院得以認定該民眾確有侮辱公務員之行為。

三、 訂定標準處理程序

對於洽公民眾可能發生之各種偶突發狀況，機關可訂定標準處理程序，從洽公動線、狀況發生、支援人力、協助單位等均應有明確的依據，其處理原則如下：

（一）先要引領民眾離開第一現場（窗口、櫃臺），倒杯水紓緩其憤怒之情緒，俟其心平氣和，再予以解釋。

（二）由後線或資深熟悉業務人員即時出面瞭解、避免衝突升高，並隔離不相干人員。

（三）誠懇、耐心、傾聽、婉轉解決對立、緩和情緒。

（四）不卑不亢、不使用刺激言語或誇張、過度肢體動作。

（五）察言觀色注意任何可能突發狀況。

（六）妥善因應衝突事件階段：潛伏、爆發、延續、善後期（可能發生不良副作用）之處理步驟。

（七）由主管、首長（副首長）最後出面斡旋緩頰，或以書面申

訴等方式結束爭執。

四、 加強員工危機意識

基層公務機關之業務與業者、民眾接觸頻繁，且與其權益息息相關，常遇有「爭執衝突」事件發生，公務員必須本諸職權依法行政，以「同理心」爭取與民眾「良性互動」，講求技巧，必能減少不必要之紛爭和困擾，另應教育宣導員工狀況處理程序，定期演練以使員工熟悉應變程 序及提升危機意識。

【資料來源：臺中市大安區公所】