AI軟體與服務可能產生之風險疑慮

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。

- **針對生成結果需進行評估後再行運用**：內容生成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。
- **應避免暴露個人資料與機敏資訊：**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。
- **留意提供該軟體與服務之公司背景**：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，因此不應盲目信任使用AI軟體與服務。

行政院及所屬機關（構）使用生成式AI參考指引

1. 為使行政院及所屬機關（構）（以下簡稱各機關）使用生成式AI提升行政效率，並避免其可能帶來之國家安全、資訊安全、人權、隱私、倫理及法律等風險，特就各機關使用生成式AI 應注意之事項，訂定本參考指引。
2. 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。
3. 製作機密文書應由業務承辦人親自撰寫，禁止使用生成式AI。前項所稱機密文書，指行政院「文書處理手冊」所定之國家機密文書及一般公務機密文書。
4. 業務承辦人不得向生成式AI 提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式AI 詢問可能涉及機密業務或個人資料之問題。但封閉式地端部署之生成式AI 模型，於確認系統環境安全性後，得依文書或資訊機密等級分級使用。
5. 各機關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行政行為或作為公務決策之唯一依據。
6. 各機關使用生成式AI 作為執行業務或提供服務輔助工具時，應適當揭露。
7. 使用生成式AI 應遵守資通安全、個人資料保護、著作權及相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。各機關得依使用生成式AI 之設備及業務性質，訂定使用生成式AI之規範或內控管理措施。

8. 各機關應就所辦採購事項，要求得標之法人、團體或個人注意本參考指引，並遵守各機關依前點所訂定之規範或內控管理措施。
9. 公營事業機構、公立學校、行政法人及政府捐助之財團法人使用生成式 AI，得準用本參考指引。
10. 行政院及所屬機關（構）以外之機關得參照本參考指引，訂定使用生成式AI 之規範。