行政院及所屬機關（構）使用生成式 AI 參考指引

近年來生成式 AI 快速發展，影響遍及全球產官學研各界。其中 ChatGPT 於 2022 年底發布後，更掀起全球熱潮，且功能極為多元，已被視為人工智慧之一項重大突破。參考歐盟之定義，生成式 AI 模型是一種電腦程式，旨在創建類似於人類製作（human-made）之新內容；其大量蒐集、學習與產出之資料，可能涉及智慧財產權、人權或業務機密之侵害，且其生成結果，因受限於所學習資料之品質與數量，有可能真偽難辨或創造不存在之資訊，須客觀且專業評估其產出資訊與風險。

考量行政院及所屬機關（構）（以下簡稱各機關）利用生成式 AI 協助執行業務或提供服務，有助於行政效率之提升，且為保持執行公務之機密性及專業性，並促使各機關使用生成式 AI 有一致之認知及基本原則，爰參考各國政府之審慎因應作法，研訂「行政院及所屬機關（構）使用生成式 AI 參考指引」（以下簡稱本參考指引），供各機關依循。各機關得視使用生成式 AI 之業務需求，參酌本參考指引另訂使用規範或內控管理措施。

衡酌 AI 發展具重要性且與資訊安全及國家安全息息相關，本參考指引明確揭示各機關人員使用生成式 AI 時，應秉持負責任及可信賴之態度，掌握自主權與控制權，並秉持安全性、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。因 AI 之發展日新月異，後續將觀察全球 AI 發展趨勢與因應作為，及各機關於人工智慧應用之推動情形，持續滾動修正本參考指引。

本參考指引共計十點如下：

一、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。

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、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。

四、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。

五、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。

六、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。

七、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。

八、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。

九、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。

十、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。