國軍使用生成式AI服務平臺注意事項

中華民國112年10月06日國通軟資字第1120273018號令頒
中華民國114年03月25日國通軟資字第1140081320號修頒

一、因應生成式人工智慧（AI）服務平臺係運用大量蒐集、學習用戶提供資訊產出各式成品，使用不慎恐涉及軍事機密、個人資料安全及侵害智慧財產權等疑慮，為確保國軍所屬人員使用合於資訊安全，訂定本注意事項。

二、國軍以軍事安全為首要，為防資料遭蒐集學習記錄，凡涉及國軍公務資訊或其他法規所限制之資訊及個人資料，嚴禁上傳至外部生成式AI服務平臺，並不得藉此平臺製作或處理各類業管公務文書。

三、國防部配合政府推動AI全面應用政策指導，於兼顧開放及安全原則下，凡屬封閉式地端部署或可管控資料限制於指定位置之生成式AI模型，於確認模型來源、系統環境安全性及無資料外洩疑慮後，得依資訊機密等級分級管制使用，以確保國軍資通安全。

四、生成式AI服務平臺有產出不正確或模糊資訊之疑慮，官兵於個人查詢參考使用前須仔細查核比對驗證，以維資料準確性。

五、嚴禁利用各類生成式AI服務平臺從事非法及違反社會善良風俗之活動，如涉及國防機密外洩或損害國軍軍譽者，依法究辦。

六、運用生成式AI服務平臺於進修教育及終生學習時，應遵守資通安全、個人資料保護、著作權與相關學術倫理規範，並注意其侵害智慧財產權之可能性。

七、各單位採購案，應將本注意事項所定納入採購契約，要求得標之法人、團體或個人遵守。

八、各單位得參照本作法，訂定所屬使用生成式AI服務平臺之規範。