公務機關不得使用 Deepseek AI 服務以防範資安風險

基於國家資通安全考量，數位發展部特別警示公務機關與關鍵基礎設施等應限制使用 DeepSeek AI產品，以避免使用者相關數據或資訊被這類有資安疑慮的產品傳送，造成危害國家資通安全的疑慮。

數位發展部表示，依行政院及所屬機關（構）使用生成式AI參考指引，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。另查DeepSeek AI 服務為中國產品，其運行涉跨境傳輸及資訊外洩等資安疑慮， 屬危害國家資通安全產品，為防範公務機關內部資訊在無法有效監管的情況下外流並構成危害風險，我國從2019年行政院公布實施「各機關對危害國家資通安全產品限制使用原則」，已明確要求中央與地方機關（構）、公立學校、公營事業、行政法人以及自行或委外營運提供公眾活動或使用之場地，限制使用危害國家資通安全產品。此外，中央目的事業主管機關應督導資通安全管理法所定關鍵基礎設施提供者及政府捐助之財團法人，參考辦理。

數位發展部強調，上班時間內不得利用電腦及網路設備從事與公務無關之行為，各機關資通安全防護至關重要，數位發展部將持續掌握相關技術發展，並適時調整資安政策，以保障國家資訊安全。

發布單位：政務次長辦公室　建立日期：2025-01-31　更新日期：2025-01-31