公務機密維護園地

私接內、外網，違反資安規定案例

壹、案情概述

一、中央部會某機關為維護資通安全，已實施內外網實體隔離，其資通安全防護管理中心於 98 年 11 月 5 日發覺所屬某單位某主機疑似內外網串接。經查，該電腦為連結內網用筆記型電腦，該單位歐○為辦理業務傳輸照片需要，因外網電腦故障無法使用，而貪圖一時之便，未經報准私自使用 3.5G 無線網卡對外網路連線進行資料上傳，且自購網路卡安裝測試連外網路，致出現防毒系統之網路攻擊警告訊息。

二、經查核該部電腦發現，係以管理者權限登入使用、未安裝資產管理系統、防毒軟體於事發後才安裝、系統漏洞未修補、曾安裝遊戲軟體及手機傳輸軟體等，存在諸多高風險問題，顯示未落實資安管理，使該設備成為資安漏洞。

三、歐○行為已違反相關資安規定，雖經檢測分析，該部電腦內並無任何機敏資料存在，且查無植入惡意程式徵兆，亦無具體事證顯示資料外洩，故對歐○予以口頭訓誡，並將該事件列入年終考績評核以示懲戒。

貳、經驗教訓

一、缺失檢討

（一）未經報准私自以無線網卡連結外網：

歐○為辦理業務，貪圖一時之便，未經報准私自使用 3.5G 無線網卡對外網路連線，且將自購網路卡攜入並將公務電腦連外網路，致出現防毒系統之網路攻擊警告訊息。

（二）未落實權限控管及安全防護作為：

本案發生肇因於該單位前資訊承辦人未落實資安管理，且新接任人員未能實施定期檢查，未將電腦管理者權限收回，使用者得以自行安裝軟體，致發生內外網串接事件。

（三）未落實資安政策及可攜式媒體管制：

事件發生當事人歐○未落實資安政策，將內、外網設備串接，因己一時之疏失，造成單位資料有外洩危機，且此舉將造成資安防護罅隙，另該單位未落實可攜式媒體管制，肇致人員攜帶行動網卡使用。

二、策進作為及建議

（一）收回電腦管理者權限，如遇更新需求時，則申請短時間開放之例外，以避免使用者自行安裝不當連線軟體。

（二）確實安裝資產管理軟體管控，關閉 USB 等可攜式媒體之連結，避免資料外洩。

（三）要求承辦人確實將筆記型電腦定期收回進行系統更新、漏洞修補、掃毒等作業，提昇安全強度。

（四）於內部網站、會議會報等實施宣導，禁止內外網串接及無線上網，落實資安政策。

（五）如有內、外網資料交換需求，應依規定程序辦理交換，落實資安管理。

參、相關法規

一、該機關可攜式資訊設備及儲存媒體管理要點第 4 點：「私人所有可攜式資訊媒體一律嚴禁使用」。

二、該機關網路使用管理要點第 5 點：「機關員工應於合法授權範圍內使用機關網路，如有下列行為之一者（未經許可，擅自於單位內以各種方式私接網際網路或串連內、外部網路，嚴重威脅機關網路安

全之行為），得停止其使用權利，情節重大者並報請其機關首長議處，若涉及違法、侵權之行為，除依相關法令追究其責任外，並檢討所屬機關（單位）網路安全管理之責」

三、刑法第 132 條：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。因過失犯前項之罪者，處一年以下有期徒刑、拘役或三百元以下罰金。」