檔　　號:
保存年限:

數位發展部 函

地址：10066臺北市中正區延平南路143號
聯絡人：許舜翔
電話：02-23808691
電子郵件：shun3915@acs.gov.tw

受文者：教育部

發文日期：中華民國115年9月1日
發文字號：數授資通字第1152000274號
速別：普通件
密等及解密條件或保密期限：
附件：

裝

主旨：為加強各機關網通設備及IoT設備對外連結之資安管理，請依說明辦理，並轉知所屬機關（構），請查照。

說明：

一、依據資通安全責任等級分級辦法第11條第2項及附表十規定辦理。

訂

二、為降低機關（構）網通設備及IoT設備因管理介面直接開放網際網路存取，或存在未修補之已知漏洞，而遭駭侵利用作為入侵管道之風險，爰請各機關（構）辦理下列事項，以強化整體資安防護。

線

(一)全面盤點對外IP位址、網域名稱及開放之通訊埠與服務，建立前揭資產清冊並指定管理權責；盤點範圍應涵蓋網通設備（如路由器、防火牆、VPN設備等）及IoT設備（如網路攝影機、網路儲存設備、印表機、環境監控設備、門禁系統、差勤設備等），並應自網際網路側檢視自身對外可見情形，確認無非預期暴露之設備或服務。

(二)網通及IoT設備之管理介面（例如Web管理頁面、SSH、

1150090119 收文日期:115/09/02

Telnet、RDP、SNMP等）不得直接開放網際網路存取；確有遠端管理需求者，應透過VPN或零信任網路存取等安全機制連線，並以存取控制清單限制可連線來源；採用之VPN設備本身亦應納入本函各項檢視範圍。

(三)應落實最小開放原則，關閉不必要之服務及通訊埠；對於必須開放之服務，應停用已知不安全或未加密之通訊協定（如Telnet、FTP、SNMP v1/v2c等），並改採用加密安全方案（如SSH、SFTP、SNMPv3等）。

(四)定期執行設備韌體及安全更新，並訂定漏洞修補時程，優先處理已遭實際利用之漏洞；已終止支援、無法取得安全更新之設備，不應繼續作為對外連線設備使用，應訂定汰換期程。

(五)變更設備出廠預設帳號密碼並設定高強度密碼；管理帳號建議啟用多因子驗證，並移除或停用不必要之帳號。

(六)IoT設備原則置於獨立網段，與核心業務系統及機敏資料網段隔離，並限制其對外連線行為。

(七)定期檢視前述各項措施之有效性（含新增設備是否納管），保存對外連線紀錄至少半年，並就異常連線建立告警機制。

(八)採購網通及IoT設備時，應將資安要求（如設備具備安全更新機制及可停用遠端連線功能等）納入採購規範；若屬小額採購等無規範書之情形，採購人員應依上述原則進行選購評估。

(九)前開設備不得為危害國家資通安全產品，包括大陸（含香港及澳門）之廠牌；各機關如因業務需要且無替代方

案，應報經數位發展部核定。

三、上開事項及委外活動網站網域管理情形（本部115年6月26日數授資通字第1152000210號函諒達）續將列入行政院資通安全稽核之稽核項目。

正本：行政院各部會行總處(不含本部)、各直轄市政府、各縣（市）政府、各直轄市議會、各縣（市）議會、本部資訊處

副本：電子公文交換章 2026/09/01 17:47:30