

臺北市政府教育局 函

地址：110204臺北市信義區市府路1號
承辦人：陳柏儒
電話：02-27208889#1235
電子信箱：as3599@gov.taipei

受文者：臺北市民族實驗國民中學

發文日期：中華民國115年9月16日
發文字號：北市教資字第1153099124號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：為加強各機關學校網通設備及IoT設備對外連結之資安管理一案，請查照。

說明：

- 一、依數位發展部（下稱數發部）115年9月1日數授資通字第1152000274號函、本府115年9月8日府授資安字第1150141659號函、資通安全責任等級分級辦法第11條第2項及附表十「資通系統防護基準」規定辦理。
- 二、為降低機關學校網通設備及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，而遭駭客利用作為入侵管道之風險，爰請各機關學校辦理下列事項，以強化整體資安防護：
 - （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、Telnet、RDP、SNMP等）禁止直接開放外部網路存取，應以內部網路存取為限；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、SNMP v3等）；如因不可抗力因素無法關閉或替換，則應禁止對外連線，僅限於內部網路存取，並擬定計畫改加密安全方案。
- (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)辦理資訊採購（含網通及IoT設備）時，應參照行政院公共工程委員會最新版本之「資訊採購範本」，並至本局KM知識管理平臺查閱最新版「資訊採購作業規範範本」，並將資安要求（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，應經本局報請數發部核定。

正本：臺北市政府教育局所屬機關、臺北市政府教育局所屬公私立各級學校（含附設國立中小學）

副本：臺北市政府教育局各科室（臺北市政府教育局資訊教育科除外）

