

美和科技大學

IoT 設備（有線/無線）連線管理規定

民國 115 年 7 月 16 日 114 學年度資訊網路發展委員會議通過

一、IoT 設備定義與適用範圍

IoT 設備（有線/無線）連線管理規定（以下稱為本規定）所指之 IoT（物聯網）設備，係指具備網路連線功能，但非屬通用型電腦（如：PC、筆電）之專門用途裝置。包含但不限於：

- (一) 監控感測類：IP 攝影機（CCTV）、溫濕度感測器、環境監測儀、NAS 儲存裝置。
- (二) 自動化控制類：PLC 控制器、工業閘道器（Gateway）、機械手臂、智慧電錶。
- (三) 辦公與生活家電類：網路印表機/複合機、網路投影機、智慧飲水機、門禁考勤機、連網空調。
- (四) 醫療與實驗設備：智慧病床、聯網實驗儀器、穿戴式量測裝置等具備網路連線功能。

辨識原則：凡「無固定操作者」、「單一特定用途」、「系統封閉（無法自行安裝軟體）」之連網裝置，皆屬本規定管理範圍。

二、入網申請與異動申報

- 1. 設備接入網路前，必須向管理單位提交申請，登記資訊包含：
 - (1) 設備資訊：廠牌、型號、MAC 位址（有線與無線網卡須分別登記）。
 - (2) 管理資訊：使用者（負責人）、所屬管理單位。
- 2. 凡屬下列情事，使用者須主動向管理單位辦理資料變更，否則將導致連線中斷：
 - (1) 設備維修：更換主機板或網卡導致 MAC 位址改變。
 - (2) 人員異動：使用者（負責人）離職、調職或變更。
 - (3) 單位移轉：設備撥交至其他管理部門。
 - (4) 設備汰換：設備報廢或永久不再使用。
- 3. 使用期限：
 - (1) 每次申請有效期為一學年。
 - (2) 使用者須於到期前一個月內主動提出續用申請。
 - (3) 逾期未辦理者，資訊圖書處將逕行從白名單剔除並收回 IP 位址。
- 4. 不開放大陸廠牌設備申請。

四、設備技術規範

1. IP 分配：一律設為「自動取得 IP (DHCP)」，嚴禁私設靜態 IP。
2. MAC 地址：必須使用硬體原始地址，務必關閉「隨機 MAC」或「私密位址」功能。
3. 無線模式：SSID 驗證模式請選擇「Open / 無加密」。

五、弱點掃描與稽核管理

4. 不定期弱掃：資訊圖書處將針對連網設備執行不定期弱點掃描 (Vulnerability Scan)，包含埠位檢測與服務弱點。
5. 改善時限：若掃描發現資安弱點 (如：使用預設密碼、不安全通訊協議)，經資訊圖書處通知後，使用者須於限期內完成修補，否則將關閉連線埠或取消無線存取權限。

六、資安事件處理

1. 強制隔離：若偵測到異常流量、中毒或攻擊行為，資訊圖書處得先行阻斷連線。
2. 現況保留：事件發生後，使用者應配合調查，嚴禁擅自重設 (Reset) 設備，以保留資安紀錄。
3. 復原審核：漏洞修補後須提供相關佐證，或直接與資訊圖書處聯繫，經資訊圖書處確認安全後，方可重新開通網路。

七、禁令與責任

1. 禁止私接：嚴禁自行串接交換器 (Switch) 或非法無線存取點 (AP)。
2. 數據加密：校園網路不提供鏈路層加密，機敏資料傳輸應使用加密協定 (如：HTTPS、TLS)。
3. 密碼規範：使用者負有維護設備安全之責，嚴禁使用設備廠牌原始預設密碼。

八、本規定經資訊網路發展委員會議通過後公告實施，修正時亦同。