

國立高雄餐旅大學

物聯網 (IoT) 設備資通安全管理作業指引

一、目的

為強化國立高雄餐旅大學（以下簡稱本校）物聯網（Internet of Things, IoT）設備之管理及資通安全防護，避免因設備弱點、預設帳號密碼、韌體漏洞、存取控制不足或不當連網等因素，造成資訊外洩、設備遭入侵、服務中斷或成為攻擊跳板等資安事件，特訂定本作業程序，以建立物聯網設備之盤點、管理、監控、更新及應變機制，確保校園網路與資訊環境之安全。

二、適用範圍

本指引適用於本校各單位所管理或使用之 IoT 設備，包括但不限於：

1. 網路攝影機。
2. 網路印表機。
3. 無線路由器。
4. 門禁控制設備。
5. 其他網路連線之資訊設備或嵌入式設備。

三、IoT 設備建置與驗收管理

各單位於 IoT 設備建置完成或驗收時，應確認設備已完成必要安全設定，包含：

1. 變更設備預設帳號密碼

應於設備啟用前修改原廠預設帳號及密碼，並依本校密碼安全政策設定具一定複雜度之強健密碼(10 碼以上)，避免遭利用預設帳號進行未授權存取。

2. 更新設備韌體版本

應確認設備已更新至製造商提供之最新穩定韌體版本，以修補已知漏洞及提升設備安全性。

3. 關閉非必要服務

應檢視設備提供之服務及功能，關閉不必要之通訊協定、服務或管理介面，以降低攻擊面。

4. 完成設備登錄及定期盤點

設備建置完成後，應納入本校資訊資產清冊管理，確保設備資訊完整可追蹤，並且應至少每年辦理一次 IoT 設備盤點作業，確認設備實際使用狀況，並依盤點結果更新資訊資產清冊。

5. 納入維護管理機制

應建立設備維護管理流程，包含韌體更新、設備檢查、異常處理及廠商維護管理等事項。

四、IoT 設備維護與安全管理

1. 本校禁止使用大陸廠牌之 IoT 設備。
2. 管理單位應定期確認設備韌體更新資訊，並依設備重要性及風險評估結果辦理更新。
3. IoT 設備如停止使用，應依資訊資產管理程序辦理停用或報廢及移除網路連線。
4. 設備管理介面應限制存取來源，避免直接暴露於外部網路。
5. IoT 設備如涉及影像、個人資料或敏感資訊蒐集，應依個人資料保護及資訊安全相關規範辦理。
6. 發現設備遭異常存取、感染惡意程式或發生資通安全事件時，應依本校資通安全事件通報及應變程序辦理。