

國立臺中教育大學

物聯網設備使用管理規範

一、適用範圍

具網路連線功能之印表機／多功能事務機、門禁系統、環境與能源管理系統、網路監視器、無線網路基地台（AP）、連網電子看板／智慧黑板／網路儲存設備（NAS）等物聯網設備（下簡稱設備）。

二、設備採購與帳號管理

- （一）依據政府資安規定，校園內禁止採購與使用中國大陸廠牌之具連網功能產品。
- （二）新設備啟用時，必須立即變更出廠預設密碼，設定複雜度高之密碼。
- （三）同型號之不同設備，嚴禁使用相同密碼。
- （四）落實帳號清查，每年檢查設備管理帳號，即時刪除離職人員或不再使用的測試帳號。

三、網路服務與通訊協定規範

- （一）設備必要時得申請實體 IP，或架設小型防火牆進行網段隔離。
- （二）應關閉設備上未使用的通訊埠並強制停用未加密且過時的遠端管理服務，如 rsh 與 telnet。
- （三）如設備具防火牆功能，應設定防火牆規則，僅允許校內特定管理 IP 登入設備後台。
- （四）如設備具 snmp 管理功能之物連網設備，必須變更 snmp 預設授權字串（禁止使用 public 或 private），以防止設備資訊外洩或遭惡意竄改設定；若無監控需求，建議直接關閉 snmp 服務。

四、漏洞管理與維護規範

- （一）對於已停止維護且無法修補中、高風險弱點的物聯網設備，應編列預算評估汰換，或採取嚴格的網路隔離措施作為補償控制。
- （二）接獲資安漏洞通報（如 TACERT 漏洞通報）時，應儘速完成清查、風險評估及修補；如已形成資安事件，依資安事件通報及應變程序辦理。
- （三）如需使用 ftp 傳輸資料時，嚴禁使用弱密碼（如 123、scan 等），請參照「ISMS-2-005 帳號密碼及存取控制管理程序

書」6.5.2 帳號密碼使用管理原則，進行相關設定，並且應定期清理儲存於物連網設備或電腦中的個資檔案。

- (四)各單位應由資安聯絡人每年填寫「物聯網設備安全檢查表」，確保所有物連網設備皆符合上述規範，以維持校園網路整體安全性。
- (五)計網中心將不定期檢測物連網設備及個人電腦資安防護情形，如有違反上述規範，將開立「ISMS-2-004-02 資通設備重大弱點補強紀錄表」，請相關人員限期改善。
- (六)設備報廢或移轉前，必須執行恢復原廠設定，並確實銷毀內部儲存之公務或個人資料。

國立臺中教育大學
物聯網設備安全檢查表

檢查日期：

物聯網設備基本資料			
設備類型： ☐ 印表機類 ☐ 門禁系統 ☐ 環控系統 ☐ 監視器 ☐ 其它：_____			
設備廠牌：			
設備型號：			
設備 IP：			
使用單位：			
檢查項目	檢查要點	檢查結果	說明
資產盤點	已納入資訊資產盤點。	☐ 符合 ☐ 不符合 ☐ 不適用	
變更預設密碼	已更改出廠預設密碼。	☐ 符合 ☐ 不符合 ☐ 不適用	
未共用密碼	同型號或同款設備，已設定不同的管理密碼。	☐ 符合 ☐ 不符合 ☐ 不適用	
帳號清查	已進行帳號清查，並刪除或停用離職人員、畢業學生或過期廠商的管理帳號。	☐ 符合 ☐ 不符合 ☐ 不適用	
限制管理來源	設備後台網頁或管理介面，已設定僅限校內特定管理 IP 或透過學校 VPN 才能登入。	☐ 符合 ☐ 不符合 ☐ 不適用	
關閉非必要通訊埠	已關閉設備上未使用的服務及 port（如：telnet、snmp v1/v2、UPnP）。	☐ 符合 ☐ 不符合 ☐ 不適用	
snmp 字串變更	snmp 社群字串已進行修改，而非使用預設值 public（唯讀）或 private（讀寫）。	☐ 符合 ☐ 不符合 ☐ 不適用	
網路存取控制	設備管理介面已限制僅限特定內部 IP 存取，而非對全網段開放。	☐ 符合 ☐ 不符合	

		☐ 不適用	
定期韌體更新	已至原廠官網確認，並將設備韌體更新至最新安全版本。	☐ 符合 ☐ 不符合 ☐ 不適用	
1. 請據實填寫，必要時計網中心將開立修補單並斷網處置，直至改善止。 2. 採購新設備後，於申請 IP 時一併繳交。 3. 各單位應於每年辦理「ISMS-2-003-06 個人電腦安全檢查表」自評時，一併完成本檢查表。			

填表人：

主管：