慈濟學校財團法人慈濟科技大學物聯網設備安全指引

中華民國 112 年 1 月 9 日
資訊安全暨個人資料保護推動委員會訂定

一、 本指引所稱物聯網設備係指處理公務具網路連線功能之設備，包含列表機(事務機)、網路攝影機(監控系統)、網路儲存設備、無線網路分享器、數位電子看板(跑馬燈)、門禁系統、智慧型人型機器人、電力系統、雲端智慧家電、IOT 開發板等。

二、 禁止使用大陸廠牌資通訊設備，例外使用應敘明理由，經本會議審核通過後，才可以購置使用，但要列冊管理且需遵守提供特定區域和特定人員使用，及不得使用公務網路環境介接、不得處理或儲存機關公務資訊。

三、 設備具備安全性更新機制者應予以更新，以維持設備之整體安全性。

四、 設備應具備身分驗證機制，不得使用廠商預設帳密及弱密碼，應變更預設帳號密碼，密碼長度應至少 8 碼，並取英文字母大小寫、數字與特殊符號其中 2 種要素之組合。

五、 設備應關閉不必要之網路連線及服務，依業務需求設定適當網路存取限制；無需對外開放連線者，得以防火牆限制僅供內部連線。

六、 各單位應建立物聯網設備管理清冊並至少每年更新一次，以利電子計算機中心識別設備網段、存放位置與管理人員，進行資安分級並評估適當之實體環境控管措施及存取權限管制。

七、 資安分級為中等級以上之設備需進行資安檢核。
檢核項目如下：
- 連線方式有線還是無線
- 登入是否需要帳號密碼
- 登入之密碼是否使用預設密碼
- 密碼是否符合資安要求
- 是否開啟不必要之連線
- 是否有安全性更新
- 是否為大陸廠牌

八、 若設備無法落實本指引第三、四、五、七條之安全控管規範，應限制網際網路連線能力，加強存取控制或進行網路連線行為監控。若設備存在已知弱點且無法修補或更新，應訂定汰換期程。

九、 物聯網設備於採購前，應依據本指引進行評估及測試，並且得優先採購取得資安標章之物聯網設備，且應與設備供應商簽訂資訊安全相關協議，其內容得包含服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關

應變處置方案等事項，以明確約定相關責任，申請採購時需標示是否為連網設備，並由電子計算機中心進行審規此設備之安全機制。

十、 本指引經資訊安全暨個人資料保護推動委員會議通過後，陳請校長公布實施，修正時亦同。