

逢甲大學物聯網管理要點

民國 109 年 08 月 12 日第 1090812(1135)次行政會議通過

民國 109 年 08 月 20 日校長核定並公布

民國 111 年 09 月 14 日第 1110914(1174)次行政會議通過

民國 111 年 09 月 16 日校長核定並公布

- 一、 資訊總處建置全校物聯網管理平台(FCU-IoT)，進行校園物聯網設備 資料收集，以利教學研究與行政應用。為有效管理校園物聯網設備 及確保校園網路與系統之資訊安全，特訂定本要點。
- 二、 本要點所指之物聯網平台，為資訊總處建置提供各單位物聯網設備資料收集與管理之系統。物聯網設備，泛指各式進行環境感測與動作觸發，且具有網路傳輸資料功能之設備，例如感測器、智慧家電、單板電腦及網路攝影機等，但不以前述設備為限。
- 三、 資訊總處為物聯網平台之管理權責單位，負責平台之運作維護及權限管理，並提供各單位物聯網設備選用與設定建議。各單位可依使用場景與需求採購所需物聯網設備，自行負責設備安裝、設定及後續管理與維護，並可依需要向資訊總處申請物聯網平台權限，利用平台開發相關應用。
- 四、 為確保物聯網設備可與物聯網平台順利介接，設備應優先採用使用 公開通用之通訊協定、提供開放應用程式介面(Open API)或其它可開放資料存取之產品，避免採用僅能透過特定應用程式控制之產品。
- 五、 各單位於校園架設物聯網設備，應以電子表單物聯網裝置連線申請表向資訊總處提出申請。資訊總處應就設備之用途及防護能力進行評估後，決定是否提供裝置連線，並依裝置特性進行相關網路限制。
- 六、 各單位可向資訊總處申請校園物聯網平台之使用權限，藉以進行裝置管理或對裝置感測數據之收集、處理與利用，並自行開發所需之相關應用。
- 七、 物聯網設備涉及提供網路管理或使用介面者，應設有帳號密碼進行 保護(密碼至少須有 12 碼)，並禁止使用設備原預設密碼。如設備提 供可限制管理者 IP 白名單功能者，亦應設定為僅允許被授權管理者 可連線操作，以確保物聯網設備不被未授權使用者盜用。
- 八、 物聯網設備管理者應隨時留意設備是否有安全性修正或新版韌體可供更新，並進行更新，以確保設備不會因自身漏洞而遭到攻擊者利用。
- 九、 如物聯網設備須透過網路傳送機敏性資料，應啟用資料加密傳輸功能，以避免資料在傳輸過程中遭竊聽而產生資料外洩或資料竄改等情形。
- 十、 如物聯網設備設置於公共或開放區域，應確保物聯網設備受到適當保護，以避免發生設備遭到破壞或被竊取等情形。
- 十一、 本要點經行政會議通過，陳請校長核定後公布實施，修正時亦同。