臺北市政府使用物聯網安全作業指引

中華民國111年2月24日臺北市政府(111)府授資安字第1113003287號函訂定發布

壹、 總則

一、 臺北市政府(以下簡稱本府)為確保所屬各機關(構)(以下簡稱各機關)使用物聯網(Internet of Things, IoT)設備及管理平台之安全性，降低相關作業風險，特訂定本指引。

貳、 名詞定義

二、 本指引所稱物聯網係指處理公務具網路連線功能並連線於 Internet 或 Intranet 之嵌入式系統(具有作業系統)設備(以下簡稱設備)，包含但不限於自動化辦公設備(如：數位錄影機、電話交換機、傳真機、錄音設備、影印機等)、不具備遠端操控介面功能之感測器等。

參、 物聯網設備安全控管

三、 各機關應建立物聯網設備管理清冊並至少每年更新一次，以識別設備用途、網段、存放位置與管理人員，評估適當之實體環境控管措施及存取權限管制。

四、 設備應具備安全性更新機制，以維持設備之整體安全性。

五、 為確保經授權之使用者始得進行資料存取、設備管理及安全性更新等操作，設備應具備身分驗證機制，並應進行初始密碼變更，密碼長度不應少於十二碼，採英數字混合使用，得包含大小寫英文字母或符號，並以最小權限原則，針對不同的使用者身分進行授權。

六、 設備以無線連接網路者，應採用具加密協定之無線存取點連接網路，並以網路卡卡號白名單等機制進行設備綁定。

七、 設備應關閉不必要之網路連線及服務，並避免使用對外公開之網際網路位置，如設備採用公開的網際網路位置，應於前端設置防火牆以防護，採用白名單方式進行存取過濾，並應辦理滲透測試、伺服器應用系統之程式原始碼掃描或黑箱測試、檢視伺服器目錄與網頁之存取權限及檢視系統是否有異常的授權連線、CPU 資源異常耗用及異常之資料庫存取行為等情況。

八、 應定期檢視設備之存取紀錄及帳號權限，識別異常紀錄與確認警示機制。

九、 設備網路安全管理應依臺北市政府網路管理規範規定辦理，並依本府資訊局訂定之相關安全基準定期稽核。

肆、 其他規定

十、 設備無法落實本指引第四、五、六、七條之安全控管規範，應建立補償性管控機制並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。

十一、 設備存在已知弱點且無法修補或更新，應依本指引第十條辦理，並視

需要訂定汰換期程。

十二、 各機關採購物聯網設備時，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。

十三、 設備於採購前應依據本指引進行評估及測試，若因業務發展需求選用無法滿足本指引要求之設備，應依本指引第十條辦理。

十四、 各機關應定期辦理物聯網設備使用及管理人員資安教育訓練。

伍、 附則

十五、 各機關得依業務需要，自行訂定其他執行管理規範。