

臺中市政府社會局

物聯網(IoT)設備資安管理規範

- 一、本規範所稱物聯網設備係指處理公務具網路連線功能之設備，包含無線網路基地台/無線路由器、監視器設備、網路印表機、門禁設備、環控系統、數位撥放器、智慧型電視、無人機……等。
- 二、使用單位應建立物聯網（IoT）設備管理清冊(附件1)，並每年5月30日前自行完成盤點作業核章備查(內部稽核抽查)，並維持管理清冊最新資訊，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。
- 三、設備軟/韌體、作業系統及相關應用程式應具備安全性更新機制，以維持設備之整體安全性。
- 四、設備應具備身分驗證機制並啟用身分鑑別功能與日誌管理功能，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，日誌記錄至少保存6個月。
- 五、設備應關閉不必要之網路連接埠及服務，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，若設備具WPS功能則須關閉。
- 六、若設備無法落實本規範第三、四、五條之安全控管規範，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。若設備存在已知弱點且無法修補或更新，應訂定汰換期程。
- 七、監視設備
 1. 設備保護與防篡改設計：攝像頭應安裝於隱蔽且不易接觸的位置，宜具備防篡改功能，且非經授權之安裝與維護人員不得進行設備操作與維修。
 2. 監視器設備要求：監視器應具備低照度夜錄功能，並確保高清晰度彩色影像錄影。監視器主機應設定校時源或定期執行校時作業，並留有紀錄。
 3. 資料管理：錄影資料保存期限依合約要求，資料應加密保存，並建立/啟用詳細的查閱與刪除紀錄，資料調閱須申請核准後才可調閱，緊急時須經機關管理人員或主管同意後始可調閱並於事後提出申請文件。
- 八、設備於採購/租賃/替換時，應依據本規範進行評估及測試，並請廠商填寫「物聯網(IoT)設備安全設定查檢表」(附件2)核章備查(內部稽核)。
- 九、採購/租賃物聯網設備時，應優先採購/租賃取得資安標章之物聯網設備或透過共同供應契約採購，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、依行政院規定，採購涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之

團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品、且該產品應取得原廠或代理商廠牌證明文件，如無法出具文件時，應由得標廠商檢附非大陸廠牌切結書，涉及雲端服務時針對委外、分包廠商(含產品原廠)，在大陸是否設置團隊據點、有否中資、產品使用是否連線經過或資料存放於陸港澳地區等議題，應請供應商於投標時說明並提供切結書(附件 3)。

十一、針對本局出租場域，應於委外契約或場地租借使用規定，明訂不得使用危害國家資安之產品（如大陸廠牌軟體、硬體及服務）。

(附件 1)

臺中市政府社會局物聯網（IoT）設備管理清冊

科室名稱：_____

外館名稱：_____

清查日期： 年 月 日

類別	項次	租賃/財產	廠牌/型號	網址 (內部IP)	放置位置 (樓層/位置)	用途	保管人	備註
網路印表機	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： _____						
門禁/考勤/ 刷卡設備	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： _____						
網路攝影機	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： _____						
無線網路基 地台/無線路 由器	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： _____						
考勤/刷卡設 備	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： _____						
智慧型電視/ 數位撥放器 (跑馬燈/看 板…)	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： _____						
無人機	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： _____						
保全設備	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： _____						

環控系統	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： 						
其他設備 (自行利用)	1	☐ 租賃 ☐ 財產 租賃廠商名稱或財編： 						
註：同一類別設備，請列在一起，項次欄位依序編號。								

承辦人：

部門主管：

(附件 2)

臺中市政府社會局

物聯網(IoT)設備安全設定查檢表

科 室：_____ 保管人員：_____

設備名稱：_____ 廠牌/型號：_____ 設 備 IP：_____

維護廠商簽名：_____ 完成日期：____年__月__日

編號	檢查項目	檢查結果	檢查說明	備註
1	有無非大陸廠牌切結書	☐ 有 ☐ 無		
2	有無雲端服務切結書	☐ 有 ☐ 缺切結書 ☐ 無使無雲端服務	是否連線經過或資料存放於陸港澳地區等議題。	
3	本機管理介面登入： ☐ 多功能事務機 ☐ 無人機 ☐ 監視主機 (DVR / NVR / XVR) ☐ 保全防盜主機 ☐ 門禁/考勤/刷卡機 ☐ 智慧電視 ☐ 數位撥放器/智慧型電視 ☐ 其他：	☐ 密碼符合規定 ☐ 空白密碼 ☐ 採預設密碼 ☐ 無啟用密碼功能 ☐ 無設定密碼功能 ☐ 弱密碼 ☐ 其他：	1. 查看有無設定登入帳號與密碼。 2. 英數混合密碼 8 碼 (含)以上。	
4	網頁管理介面登入： ☐ 多功能事務機 ☐ IP Cam ☐ 監視主機 (DVR / NVR / XVR) ☐ 門禁/考勤/刷卡機 ☐ 智慧電視 ☐ 數位撥放器/智慧型電視 ☐ 其他：	☐ 已關閉網頁服務 ☐ 密碼符合規定 ☐ 空白密碼 ☐ 採預設密碼 ☐ 無啟用密碼功能 ☐ 無設定密碼功能 ☐ 弱密碼 ☐ 其他：	1. 查看有無設定登入帳號與密碼。 2. 英數混合密碼 8 碼 (含)以上。	
5	多功能事務機掃描檔案傳輸方式： 關閉 MAIL 傳輸方式以及移除 IP 之網路開道設定。	☐ 是 ☐ 否 ☐ 無此功能	檢查掃描檔案傳輸設定是否關閉 MAIL 傳輸方式及只能在內部區域網路使用。	
6	物聯網(IoT)設備關閉 Wi-Fi 連接方式	☐ 是 ☐ 否 ☐ 無此功能	關閉無線網路支援功能設定值。	
7	啟用日誌管理功能 (保存記錄6個月)	☐ 是 ☐ 否 ☐ 無此功能	記錄設備所發生之重要事件或警示。	
8	設備具 WPS 功能則須關閉	☐ 是 ☐ 否 ☐ 無此功能	無線網路基地台/路由器	
9	關閉不必要之網路 連接埠與服務	☐ 是 ☐ 否 ☐ 無此功能	限制其對網際網路不 必要之網路連線；並避免 使用對外公開之網際網 路位置	

10	時間校時源	☐外部 ☐內部 IP：_____ ☐手動校時 日期：_____ ☐無此功能	檢查有無設定時間校時源，如果手動校時	
----	-------	--	--------------------	--

切 結 書（範例）

本廠商_____參與（招標機關）辦理（標的名稱）招標案，對於廠商之責任，包括刑事、民事與行政責任，已充分瞭解相關之法令規定，並願確實遵行，簽結承諾事項如下：

1、本公司目前是否有中國大陸地區廠商或人民持股情形？

本公司無中國大陸地區廠商或人民持股情形。

有中國大陸地區廠商或人民持股情形，其佔比情形及相關說明如下：

2、本公司及涉及本案之分包廠商是否為中國大陸地區廠商？

本公司非屬中國大陸地區廠商。

本公司非屬中國大陸地區廠商，涉及本案之分包廠商屬中國大陸地區廠商。

本公司及涉及本案之分包廠商皆非屬中國大陸地區廠商。

有中國大陸地區廠商，說明如下：

3、執行本案之團隊成員是否有中國大陸國籍人士（多重國籍者，若有屬中國大陸國籍者亦屬之）？

執行本案之團隊成員皆無陸籍人士。

本案之團隊成員有陸籍人士，說明如下：

4、本公司及涉及本案之分包廠商，是否於中國大陸地區(含香港、澳門)設立相關團隊據點？如是，則該據點與本案履約間之關係為何？

否，本公司及涉及本案之分包廠商，皆未於中國大陸地區設立相關團隊據點。

是，該據點與本案履約間之關係，說明如下：

5、本公司針對本案所提供機關(共用)產品或服務之所屬一切資料存取、備份及備援之實體所在地是否有置於中國大陸地區(含香港、澳門)之情形？或跨該等境內傳輸相關資料？

否，本公司針對本案所提供機關(共用)產品或服務之所屬一切資料存取、儲存、備份及備援等作業，皆無置於中國大陸地區(含香港、澳門)之情形，且未經該等境內傳輸相關資料。

是，有置於中國大陸地區(含香港、澳門)或該等境內傳輸相關資料，說明如下：

投標廠商：

（簽名蓋章）

負 責 人：

（簽名蓋章）

中華民國 年 月 日