112年度「民生公共物聯網資料應用補助」
資通安全要求說明

112 年 9月 5日

大綱

- 資通安全要求依據
- 資通安全自評與查核流程
- 資通安全要求條文設計
- 「提案階段」資安管理規劃
  - 資安自評表勾選
  - 資安經費規劃
- 「計畫執行階段」資安要求
- 【資安小單元】雲端平台租賃之資安要求
- 問題與討論
- 附錄
  - 資安要求條文

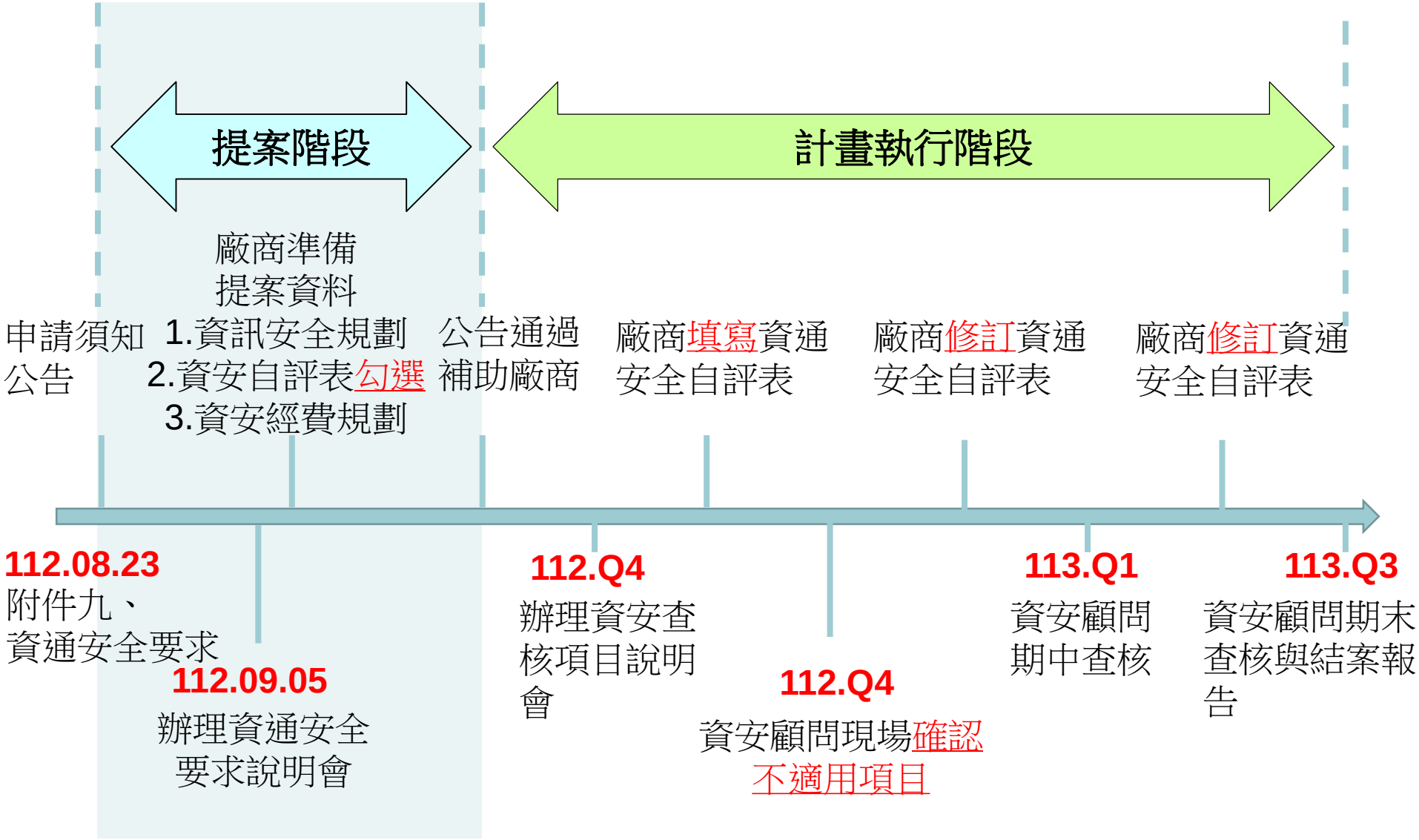
資通安全要求依據

- 依據109年6月22日「建構民生公共物聯網計畫」發行之「民生公共物聯網資通安全要求(03版)」，制定「普及與深化民生公共物聯網資料應用計畫」 辦理民生公共物聯網資料應用補助案所需之資通安全要求項目。
  - 申請須知：附件九、資通安全要求
  - 申請須知：資通安全自評表

大綱

- 資通安全要求依據
- 資通安全自評與查核流程
- 資通安全要求條文設計
- 「提案階段」資安管理規劃
  - 資安自評表勾選
  - 資安經費規劃
- 「計畫執行階段」資安要求
- 【資安小單元】雲端平台租賃之資安要求
- 問題與討論
- 附錄
  - 資安要求條文

資通安全自評與查核流程



大綱

- 資通安全要求依據
- 資通安全自評與查核流程
- 資通安全要求條文設計
- 「提案階段」資安管理規劃
  - 資安自評表勾選
  - 資安經費規劃
- 「計畫執行階段」資安要求
- 【資安小單元】雲端平台租賃之資安要求
- 問題與討論
- 附錄
  - 資安要求條文

資通安全要求條文設計

- 民生公共物聯網系統架構
- 資安要求框架
- 資安完備度

民生公共物聯網系統架構

資安要求框架

領域\原則	P1.預設就應安全	P2.資安防禦縱深	P3.可歸責性	P4.恢復能力
D1.安全功能保護	使用安全的數位簽章	使用硬體信任根	確保更新的完整性	具備援/備份能力
D2.身份辨識與認證	使用相互認證	使用多因子認證	紀錄登入失敗日誌	適當的身分管理
D3.網路管理	連接最小化	使用防火牆與VPN	記錄連線授權失敗日誌	妥善的網路區隔
D4.資料安全	啟用資料加密	保護資料之傳輸，使用及儲存	紀錄存取機敏資料	定期備份資料
D5.存取控制	實體存取限制	異常通報機制	異常日誌紀錄	防竄改機制
D6.加密保護	使用業界公認的加密方式	運用對稱或非對稱金鑰保護	合適的密鑰管理	使用完全前向保密(PFS)協定
D7.資安管理	強制使用強密碼	限制遠端對安全網路的存取	密鑰管理的職責分離	保持軟體/韌體更新
D8.營運持續	加密備份	自我檢測	監控及偵測容量使用情況	進行備援或備份之復原演練
D9.安全稽核	啟用日誌紀錄	加密日誌資料	限制對日誌之存取	定期備份日誌
D10.生命週期保護	採用系統強化基準	進行安全檢測	適當情資分享	設備再重新或汰除前清除資料

資安完備度

- 本要求的查驗結果呈現方式將導入資安完備度的評分機制(計畫結案時由資安顧問評核)

	不適用	排除	不符合	符合 Baseline	有整體管理能力	異常管理能力	持續改善能力
完備度得分	NA	EXC (1分)	0	1	2	3	4
完備度說明	因功能及成本考量難以達成判為不適用。	經風險評鑑後具合理原因能排除本項資通安全要求，並獲計畫主持人同意。	未能滿足資通安全要求，或部分未能達到要求。	達到資通安全基本要求。	已符合1分要求，並具整體性/集中化/監控性能力。	已符合2分要求，並針對/警/故報/進行通理能告異事管理力。	已符合3分要求，上述運行完善，並納入計畫整體政策與管理機制，定期接受檢查/稽核，並對發現事項/高風險事項進行有效控管。

大綱

- 資通安全要求依據
- 資通安全自評與查核流程
- 資通安全要求條文設計
- 「提案階段」資安管理規劃
  - 資安自評表勾選
  - 資安經費規劃
- 「計畫執行階段」資安要求
- 【資安小單元】雲端平台租賃之資安要求
- 問題與討論
- 附錄
  - 資安要求條文

1.資訊安全規劃

- 說明系統建置及未來系統維運時，所採用的資訊安全規劃、控制措施及個資保護等資安管理項目

資安要求條文

– 共200項 –

:應符合 153項　:原則上應符合 45項　: 不適用 2項

領域	D1 安全功能保護				D2 身份辨識與認證				D3 網路管理				D4 資料安全				D5 存取控制				D6 加密保護				D7 資安管理				D8 營運持續				D9 安全稽核				D10 生命週期保護			
條文規範	P1 使用安全的數位簽章	P2 使用硬體信任根	P3 確保更新的完整性	P4 具備援/備份能力	P1 使用相互認證	P2 使用多因子認證	P3 紀錄登入失敗日誌	P4 適當的身分管理	P1 連接最小化	P2 使用防火牆與VPN	P3 記錄連線授權失敗日誌	P4 妥善的網路區隔	P1 啟用資料加密	P2 保護資料之傳輸，使用及儲存	P3 紀錄存取機敏資料	P4 定期備份資料	P1 實體存取限制	P2 異常通報機制	P3 異常日誌紀錄	P4 防竄改機制	P1 使用業界公認的加密方式	P2 運用對稱或非對稱金鑰保護	P3 合適的密鑰管理	P4 使用完全前向保密(PFS)協定	P1 強制使用強密碼	P2 限制遠端對安全網路的存取	P3 密鑰管理的職責分離	P4 保持軟體/韌體更新	P1 加密備份	P2 自我檢測	P3 監控及偵測容量使用情況	P4 進行備援或備份之復原演練	P1 啟用日誌紀錄	P2 加密日誌資料	P3 限制對日誌之存取	P4 定期備份日誌	P1 採用系統強化基準	P2 進行安全檢測	P3 適當情資分享	P4 設備再重新或汰除前清除資料
應用程式																																								
後台伺服器																																								
網路																																								
IOT閘道器																																								
感知設備																																								

資安要求符號說明

- 資通訊系統(系統、設備、IoT裝置等)適用資通訊系統資安要求之符號說明：

●：應符合。 (✓)：原則上應符合，但依計畫風險評估後可決定適用或排除，且須經計畫主持人簽核。 ○：不適用。

2.勾選自我評核&「不適用」原因說明

自評項目		項目說明	適用設備與系統	自我評核				佐證資料說明	顧問查核結果			
				符合	部分符合	不符合	不適用		符合	部分符合	不符合	不適用
D1 安全功能保護												
D1P1 使用安全的數位簽章	資通訊系統啟動時其載入的軟體、韌體都經過完整性驗證，確保系統安全啟動，防止被植入惡意程式。	應包含開機時確認軟體、韌體完整性的自我測試相關說明。 感知設備與 IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。	1.(✓)感知設備									
			2.(✓)IoT 閘道器									
			3.●網路									
			4.●後台伺服器									
			5.●應用程式									
D1P2 使用硬體信任根	應建立硬體式的信任根（Root-of-Trust）或安全啟動的機制。	感知設備與 IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。	1.(✓)感知設備									
			2.(✓)IoT 閘道器									
			3.●網路									
			4.●後台伺服器									
			5.●應用程式									
D1P3 確保更新的完整性	具有安全措施以確保更新軟體與韌體的完整性和可信度(Trust	確認軟韌體的更新機制及作法。	1.●感知設備									
			2.●IoT 閘道器									
			3.●網路									

若勾選「不適用」需填寫原因

範例1. 廠商勾選不適用–「原則上應符合」

自評項目	項目說明	適用系統與設備	自我評核				佐證資料說明
			符合	部分符合	不符合	不適用	
D7 資安管理							
D7P1 強制使用強密碼	應建立密碼管理機制，系統應審核所使用之密碼強度，並提供密碼恢復及重置機制，管理機制包含： 1.須更改初始密碼，並不允使用硬編碼之密碼或存在管理後門密碼。 2. …..(共5項要求)	各計畫依其特性評估是否排除適用。 如有使用密碼，密碼管控應至少須包含但不限於左述幾種。	1.(✓)感知設備				V	本設備不提供使用者登入功能
			2.(✓)IoT 閘道器				V	只有符合部分強密碼原則，考量成本因素決定排除
			3.●網路		V			
			4.●後台伺服器	V				
			5.●應用程式	V				

填寫「不適用」原因

範例2：檢視勾選不適用 – 「應符合」

自評項目	項目說明	適用系統與設備	自我評核				佐證資料說明
			符合	部分符合	不符合	不適用	
D10 生命週期保護							
D10P2 進行安全檢測	資通訊系統須於上線前及營運期間定期進行弱點掃描及滲透測試，高風險漏洞應被評估並依計畫可接受方式處理。	資通訊系統須於上線前進行弱點掃描及滲透測試，且訂定合適的資安檢測週期，並對發現之威脅與弱點採取對應之預防或應變措施。	1.●感知設備				V	考量功能與成本後決定不進行弱點掃描與滲透測試
			2.●IoT 閘道器				V	考量功能與成本後決定不進行弱點掃描與滲透測試
			3.●網路	V				
			4.●後台伺服器	V				
			5.●應用程式			V		

填寫「不適用」原因。原為「應符合」項目，排除原因於計畫執行階段需能被審核委員接受

3.資安經費規劃

－ 至少佔計畫總經費 7% －

資安項目	內容說明	適用設備與系統	適用資安條文	支出費用(千元)	佔總經費比率
		( ) 感知設備			
		( ) IoT 閘道器			
		( ) 網路			
		( ) 後台伺服器			
		( ) 應用程式			
		( ) 感知設備			
		( ) IoT 閘道器			
		( ) 網路			
		( ) 後台伺服器			
		( ) 應用程式			
教育訓練(必填)		X	必要項目		
合計					

(範例)資安經費規劃

資安項目	內容說明	適用設備與系統	適用資安條文	支出費用(千元)	佔總經費比率
(範例1) 單網域SSL憑證(1年)	XX資訊應用服務系統https加密傳輸使用	( ) 感知設備 ( ) IoT 閘道器 ( ) 網路 ( ) 後台伺服器 (V) 應用程式	D4P2 保護資料之傳輸，使用及儲存	15	X %
(範例2) 網站弱點掃描(WebVA)-遠端服務(1個URL)	XX資訊應用服務軟體-Web網頁弱點掃描(遠端服務)	( ) 感知設備 ( ) IoT 閘道器 ( ) 網路 ( ) 後台伺服器 (V) 應用程式	D10P2 進行安全檢測	9.596 以【109/10/20~110/10/19電腦軟體共同供應契約-資通安全服務】收費標準為例	Y%
教育訓練(必填)	(範例3) 資安攻防技術、程式開發安全、資安稽核、ISMS(ISO27001)、法令法規(資通安全管理法、個資法)….	X	必要項目		Z%
合計(X+Y+Z)					7%

大綱

- 資通安全要求依據
- 資通安全自評與查核流程
- 資通安全要求條文設計
- 「提案階段」資安管理規劃
  - 資安自評表勾選
  - 資安經費規劃
- 「計畫執行階段」資安要求
- 【資安小單元】雲端平台租賃之資安要求
- 問題與討論
- 附錄
  - 資安要求條文

計畫資安全景

－ 均為必要執行項目 －

- 資產清冊
- 資通訊系統架構圖
- 風險評估
- 教育訓練
- 通報機制
- 法律遵循
- 委外管理
- 持續管理

資產清冊

- 民生公共物聯網之所有資訊系統與 IoT 設備應進行盤點並造冊
  - 標示其防護等級(高/中/普)

資通訊系統架構圖

- 計畫應提供其民生公共物聯網之資通訊系統架構圖
  - 說明或示意相關系統與物聯網設備間之關聯性
  - 標示或說明 IoT 資料流向

風險評估

- 本民生公共物聯網資通安全要求原則上應全部遵循
- 考量民生公共物聯網之多樣性與特性不同，各計畫可在「可選項條文要求」(以(✓)為示)，透過風險評估方式進行適用或排除之判斷
  - 評估結果之說明須經由各計畫主持人核定

教育訓練

- 計畫相關管理或日常維運人員(含委外廠商)應於每年資通安全教育課程中涵蓋 IoT 與安全軟體開發(SSDLC)等資安議題
  - 請計畫提供相關佐證資料

通報機制

- 本計畫範圍內若曾發生資安事件
  - 請計畫提供資安事件通報及處理之相關紀錄

法律遵循

- 計畫之所有資通訊相關系統與 IoT 設備應遵循我國法令法規之相關規範辦理，例如:
  - 資通安全管理法
  - 個人資料保護法
  - 智慧財產權

委外管理

- 建議各計畫於委外選商時可納入評估承攬廠商之資安完備度，例如:
  - 委外時對廠商的資通安全評估
  - 委外廠商是否建置 ISMS 資通安全管理制度，並通過第三方驗證稽核
- 若計畫有進行委外廠商之資通安全進行適度管理或稽核，請提供相關資料以備查

持續管理

- 計畫應說明何時將其民生公共物聯網範圍內之所有資通訊系統(IT、物聯網設備)納入計畫之資通安全政策
- 執行相關安控措施
- 定期接受外部稽核

1.先由資安顧問確認不適用項目

自評項目	項目說明	適用系統與設備	自我評核				佐證資料說明
			符合	部分符合	不符合	不適用	
D7 資安管理							
D7P1 強制使用強密碼	應建立密碼管理機制，系統應審核所使用之密碼強度，並提供密碼恢復及重置機制，管理機制包含： 1.須更改初始密碼，並不允使用硬編碼之密碼或存在管理後門密碼。 2. …..(共5項要求)	各計畫依其特性評估是否排除適用。 如有使用密碼，密碼管控應至少須包含但不限於左述幾種。	1.(✓)感知設備				V	本設備不提供使用者登入功能，經風險評估後決定排除
			2.(✓)IoT 閘道器				V	只有符合部分強密碼原則，經風險評估後決定排除
			3.●網路		V			僅符合部分強密碼原則
			4.●後台伺服器	V				完全符合強密碼原則
			5.●應用程式	V				完全符合強密碼原則

＊【不適用】項目先由取得補助廠商勾選（含:原因）再由資安顧問確認與調整

2.計畫執行期間依據現況填寫佐證資料

- （確認執行狀況，逐案與開期中2期末查核

自評項目	項目說明	適用系統與設備	自我評核				佐證資料說明
			符合	部分符合	不符合	不適用	
D10 生命週期保護							
D10P2 進行安全檢測	資通訊系統須於上線前及營運期間定期進行弱點掃描及滲透測試，高風險漏洞應被評估並依計畫可接受方式處理。	資通訊系統須於上線前進行弱點掃描及滲透測試，且訂定合適的資安檢測週期，並對發現之威脅與弱點採取對應之預防或應變措施。	1.●感知設備				V	經風險評估後計畫主持人決定不需進行弱點掃描與滲透測試
			2.●IoT 閘道器				V	經風險評估後計畫主持人決定不需進行弱點掃描與滲透測試
			3.●網路	V				已定期執行弱點掃描與滲透測試(可提供測試報告)
			4.●後台伺服器	V				已定期執行弱點掃描與滲透測試(可提供測試報告)
			5.●應用程式			V		開發中，尚未進行安全檢測

＊【部分符合/不符合】項目於計畫執行期間持續改善，結案前改善至【符合】

大綱

- 資通安全要求依據
- 資通安全自評與查核流程
- 資通安全要求條文設計
- 「提案階段」資安管理規劃
  - 資安自評表勾選
  - 資安經費規劃
- 「計畫執行階段」資安要求
- 【資安小單元】雲端平台租賃之資安要求
- 問題與討論
- 附錄
  - 資安要求條文

【資安小單元】雲端平台租賃之資安要求

雲端平台供應商不會幫忙做的資安措施

- 租賃雲端平台
  - 於雲端平台(AWS、GCP、Azure...)租賃虛擬主機做為本計畫的後台伺服器，利用雲端平台供應商所提供的資安防護機制 (Firewall/IPS/WAF…)保護該伺服器
- 供應商不會幫忙做的資安措施：(以「五層式」民生公共物聯網系統架構分類，並以「附件九、資通安全要求」為依據)
  - 應用軟體
    - 應用軟體(含:API)是否存在OWASP Top10 Risk? 是否使用HTTPS? 是否有保存AP Log? Log保存多久? 是否使用第三方具有弱點的套件? 敏感性資料(如:密碼)是否有加密儲存?
  - 後台伺服器
    - 作業系統(Windows、Linux…)是否存在已知弱點? 應用服務(IIS、Apache、Nginx…)是否存在已知弱點? 服務是否有最小化安裝? 系統資源(容量)是否有監控? 系統Log是否有保存? 是否有設定NTP校時? SSL憑證是否有更新? 是否定期備份? 系統發生異常應通知誰?
  - 網路
    - 虛擬防火牆網路連線政策(Firewall Policy)是否有妥善設定? 網路與資安設備的Log是否有保存? 是否有即時分析Log了解伺服器與應用軟體被攻擊的現況? 攻擊告警機制應

大綱

- 資通安全要求依據
- 資通安全自評與查核流程
- 資通安全要求條文設計
- 「提案階段」資安管理規劃
  - 資安自評表勾選
  - 資安經費規劃
- 「計畫執行階段」資安要求
- 【資安小單元】雲端平台租賃之資安要求
- 問題與討論
- 附錄
  - 資安要求條文

問題與討論

資安諮詢窗口

- 民生公共物聯網資料應用補助

  工研院　資訊與通訊研究所

  廖文全

  03-5914536

  E-mail: liao@itri.org.tw

大綱

- 資通安全要求依據
- 資通安全自評與查核流程
- 資通安全要求條文設計
- 「提案階段」資安管理規劃
  - 資安自評表勾選
  - 資安經費規劃
- 「計畫執行階段」資安要求
- 【資安小單元】雲端平台租賃之資安要求
- 問題與討論
- 附錄
  - 資安要求條文

D1 安全功能保護

D1 安全功能保護			
要求編號	要求條文	適用設備與系統	備註
D1P1 使用安全的數位簽章	資通訊系統啟動時其載入的軟體、韌體都經過完整性驗證，確保系統安全啟動，防止被植入惡意程式。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	應包含開機時確認軟體、韌體完整性的自我測試相關說明。 感知設備與 IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。
D1P2 使用硬體信任根	應建立硬體式的信任根 (Root-of-Trust) 或安全啟動的機制。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	感知設備與 IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。
D1P3 確保更新的完整性	具有安全措施以確保更新軟體與韌體的完整性和可信度(Trust and Integrity Management)。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	確認軟韌體的更新機制及作法。
D1P4 具備援/備份能力	需設計遠端異地或同地的備援或備份機制。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	計畫依資通訊系統的重要性或受衝擊的影響性來考量備份或備援機制，可採用同地或異地方案，系統具功能上的備援或備份設計即可符合。

D2 身份辨識與認證

D2 身份辨識與認證			
要求編號	要求條文	適用設備與系統	備註
D2P1 使用相互認證	在建立連線之前和預先定義的時間區間後應建立單向或雙向的被確認的機制。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	設備應有識別的機制，無論是監控或被監控。
D2P2 使用多因子認證	依照資通安全管理法中防護需求分級為高的資通訊系統，對帳號之網路或本機存取採取多重認證技術。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	依據資安法要求，資產清冊安全等級盤點為高的資通訊系統則必須採用多重認證技術。
D2P3 記錄登入失敗日誌	日誌紀錄的內容應該有人、事、時、地、物。如內容包括使用者識別碼、登入登出之日期時間、電腦/行動裝置/設備的識別資料或其 IP、修改項目、結果等事項。尤其是在登入失敗時應有日誌可以查詢。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	應注意日誌內容與完整性保存是否符合證據力與證明能力，惟每個設備若登入失敗應有日誌紀錄。
D2P4 適當的身分管理	帳號管理(含特權帳號)須能依不同角色設定不同存取權限，帳號密碼需可由設備使用者自行變更與修改，若同仁職務異動或離職時帳號權限須即時更新、鎖定或刪除。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	應有功能可以讓設備使用者自行更改密碼，帳號清冊須定期審查。 感知設備與 IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。

D3 網路管理

D3 網路管理			
要求編號	要求條文	適用設備與系統	備註
D3P1 連接 小化	網路連線需最小化，包含： 1.設備應關閉或停用不必要的通訊功能或模組。 2.應禁止非必要之網路連線。 3.僅開放網路連線必須使用的服務埠。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	網路連線應僅開放必要作業之連線或通訊模組，非必要的功能應關閉或禁用，若使用或有開放應說明開放之通訊功能或模組的必要性。
D3P2 使用防火牆與 VPN	須有防火牆、入侵偵測等資安設備保護，若透過遠端連線進行管理則必須透過加密通道，登入時必須採用安全的身分鑑別機制。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	請受查驗計畫提供網路架構圖，簡述防禦機制是否合理跟恰當。 感知設備與 IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。
D3P3 記錄連線授權失敗日誌	在連線授權失敗時應有日誌紀錄。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	感知設備與 IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。
D3P4 妥善的網路區隔	網路應進行適當的隔離，例如使用下列措施： 1.使用 VLAN。 2.對 DMZ 使用防火牆。 3.使用單向安全閘道器。 4.實體隔離。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	應描述資通訊系統的採用的網路隔離措施，而網路隔離措施必須確保能有效保護資通訊系統。

D4 資料安全

D4 資料安全			
要求編號	要求條文	適用設備與系統	備註
D4P1 啟用資料加密	對於資通訊系統中的資料應評估決定是否採取加密保護措施。	(✓) 感知設備 (✓) IoT 閘道器 (✓) 網路 (✓) 後台伺服器 (✓) 應用程式	計畫應評估資通訊系通那些需要加密保護，加密方式以 D6 要求為依據。 各計畫依其特性評估是否排除適用。
D4P2 保護資料之傳輸，使用及儲存	若存在機敏性資料時，無論傳輸、使用和儲存都應進行加密保護。	(✓) 感知設備 (✓) IoT 閘道器 (✓) 網路 (✓) 後台伺服器 (✓) 應用程式	若資通訊系統中有機敏性資料，則在傳輸、使用和儲存都須採行適當之加密，加密方式以 D6 要求為依據。 各計畫依其特性評估是否排除適用。
D4P3 記錄存取機敏資料	針對機敏性資料的存取應控管並留存相關日誌紀錄。	(✓) 感知設備 (✓) IoT 閘道器 (✓) 網路 (✓) 後台伺服器 (✓) 應用程式	各計畫依其特性評估是否排除適用。
D4P4 定期備份資料	應對資料進行備份。	○ 感知設備 ○ IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	資通訊系統之資料應定期備份，可依計畫資通訊系統之特性合理訂定。 感知設備、IoT 閘道器、可能因為功能考量為不適用。

D5 存取控制

D5 存取控制			
要求編號	要求條文	適用設備與系統	備註
D5P1 實體存取限制	應有實體安全的保護措施，外連線端口需最小化管理機制。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	資通訊系統是否有該資產實體保護或操作保護機制。
D5P2 異常通報機制	若服務發生異常時(包含但不限於服務中斷、更新失敗)，需有通知管道或機制。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	資通訊系統發生異常時須要有通知機制。
D5P3 異常日誌紀錄	針對資通訊系統的異常狀況應有日誌紀錄。異常狀況可參考下列所示： 1.使用者登錄，註銷和失敗的身份驗證嘗試。 2.連接，中斷連線、連線嘗試失敗。 3.授權存取失敗。 4.存取機敏性資料。 5.從可移動媒體存取資料。 6.帳號權限的任何更改。 7.使用者新建、修改和刪除資料。 8.任何對系統變更的操作。 9.任何遠端操作。 10.安全更新失敗。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	計畫應就資通訊系統的異常狀況有所留存日誌以便日後查詢與分析。
D5P4 防竄改機制	應確保資通訊系統內的資料(設定檔、程式碼、資料庫等)不被未經授權的篡改。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	應有機制確保未經授權的人員篡改。

D6 加密保護

D6 加密保護			
要求編號	要求條文	適用設備與系統	備註
D6P1 使用業界公認的加密方式	對於設備或系統中所採用的加密機制，應採用公開、國際機構驗證且未遭破解之演算法進行保護，如使用RSA2048、AES256。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	針對加密的機制應採用公開、國際機構驗證的演算法，若因資通訊設備特殊採用非公開加密機制應說明原因。 所採用的加密演算法須為到目前為止未遭破解。
D6P2 運用對稱或非對稱金鑰保護	對於機敏性資料，應使用對稱或非對稱金鑰保護機制，對外服務之網頁憑證須由受信任憑證機構所發行或簽章。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	各計畫依其特性評估是否排除適用。
D6P3 合適的密鑰管理	須建立合適的金鑰管理機制，確保金鑰產生、儲存、使用、備份、銷毀、更新、復原等流程之安全性。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	各計畫依其特性評估是否排除適用。
D6P4 使用完全前向保密(PFS)協定	若資通訊系統有採用加密機制，應採用完全前向保密(PFS)協定，如TLS 中的 DHE-RSA、ECDHERSA、DHE-DSS 演算法，以避免金鑰被洩漏影響過去加密資料的安全性。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	各計畫依其特性評估是否排除適用。

D7 資安管理(一)

D7 資安管理			
要求編號	要求條文	適用設備與系統	備註
D7P1 強制使用強密碼	應建立密碼管理機制，系統應審核所使用之密碼強度，並提供密碼恢復及重置機制，管理機制包含： 1. 須更改初始密碼，並不允使用硬編碼之密碼或存在管理後門密碼。 2.應要求密碼強度(至少包含長度、複雜度、密碼週期)，可參考 NIST、OWASP 及 SANS 之密碼規範。 3.密碼失效鎖定機制(3 次密碼輸入錯誤即鎖定，至少 15 分鐘後解鎖)。 4.密碼需加密保存。 5.進行認證時，密碼不應以明碼方式直接顯示於畫面中。	(✓) 感知設備 (✓) IoT 閘道器 (✓) 網路 ● 後台伺服器 ● 應用程式	各計畫依其特性評估是否排除適用。 如有使用密碼，密碼管控應至少須包含但不限於左述幾種。
D7P2 限制遠端對安全網路的存取	對於遠端連線應實施適當的存取管制，至少包含使用加密方式通訊、依工作性質給予 低權限權、應保留遠端連線日誌。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	若有遠端連線應有適當的管理機制，應包含不限於連線加密方式、使用者帳號權限小化、遠端連線應留存相關日誌。
D7P3 密鑰管理的職責分離	對於金鑰的產生、儲存與使用應保存日誌紀錄，宜採用職責分離方式管理金鑰。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	對於金鑰的產生、儲存與使用應有留存日誌紀錄。其管理方式建議使用職責分離方式。

D7 資安管理(二)

D7 資安管理			
要求編號	要求條文	適用設備與系統	備註
D7P4 保持軟體/韌體更新	資通訊系統應建立軟體、韌體安全性更新機制及部署時機，若更新部署失敗應可成功回復至前一個版本。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	軟韌體更新應有安全機制以確保更新檔案的完整性。 若更新失敗應可回復前一個正常版本。

D8 營運持續

D8 營運持續			
要求編號	要求條文	適用設備與系統	備註
D8P1 加密備份	應識別重要的應用程式、設定檔、機敏資料並進行加密備份。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	應識別出資通訊清冊中那些為重要應用程式(如程式碼、函式庫)、設定檔、機敏資料(如個資等)。識別出的重要檔案應進行備份並且加密保護。 各計畫依其特性評估是否排除適用。
D8P2 自我檢測	資通訊系統應建立自我檢測功能，如完整性檢查、定期回報、零組件異常偵測，若發生上述情況時應有發送通知機制。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	資通訊系統須有檢測的機制，依各計畫資通訊系統特性訂定適合之機制，若檢測發生計畫之認為異常情況須有發送的通知機制。
D8P3 監控及偵測容量使用情況	應監控全資通訊系統使用狀況，如：CPU、記憶體、儲存空間、頻寬使用率...等，若達到警戒值應存日誌紀錄並進行通知。全資通訊系統需符合計畫自訂的可用性百分比。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	全資通訊系統的資源使用狀況都須被監控，若達到警戒值則必須通知並留存日誌紀錄，日誌存放位置不限於特定設備。只要有機制或設備進行監控所有設備的容量管理(如：達到警戒值有紀錄且通知、設備的可用性百分比...)
D8P4 進行備援或備份之復原演練	應建立業務持續運作計畫(BCP)或災難復原計畫(DRP)，定期進行演練並持續改善。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	對於資通訊系統應有BCP或DRP計畫(至少一個)。且須有定期演練紀錄，針對演練之過程缺失持續改善。

D9 安全稽核

D9 安全稽核			
要求編號	要求條文	適用設備與系統	備註
D9P1 啟用日誌紀錄	資通訊系統應進行標準時間源校時並啟用日誌紀錄功能，日誌保存期限至少5年(含)以上。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	日誌存放的相關設備對時的效時主機應該統一，以確保系統日誌時間的一致性。 感知設備與IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。
D9P2 加密日誌資料	應對日誌內容進行評估，對機敏性日誌進行加密。	(✓) 感知設備 (✓) IoT 閘道器 (✓) 網路 (✓) 後台伺服器 (✓) 應用程式	日誌內容若牽涉到機敏資料，如：個資等就應進行加密保存。 各計畫依其特性評估是否排除適用。
D9P3 限制對日誌之存取	資通訊系統內日誌存取應建立適當的存取控管，確保日誌內容不受修改、刪除、破壞及敏感資料之洩露。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	日誌存取無論在傳輸或儲存應有適當的控管機制，僅有授權的人可以存取，以避免日誌受到不當洩漏或破壞。
D9P4 定期備份日誌	須定期對日誌進行備份，並對備份日誌提供適當的保護措施。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	計畫須訂定日誌備份週期，並對備份日誌提供適當的保護措施。

D10 生命週期保護

D10 生命週期保護			
要求編號	要求條文	適用設備與系統	備註
D10P1 採用系統強化基準	資通訊系統應依據資通安全責任等級分級辦法之相關規定辦理評估資通系統分級，並依資通系統防護基準執行控制措施。	(✓) 感知設備 (✓) IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	資通訊系統應依盤點清冊的安全等級並應實施相關安控措施，以符合資安法對資通訊系統之防護基準要求。 感知設備與 IoT 閘道器可能因為功能及成本考量賦予計畫評定是否排除適用。
D10P2 進行安全檢測	資通訊系統須於上線前及營運期間定期進行弱點掃描及滲透測試，高風險漏洞應被評估並依計畫可接受方式處理。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	資通訊系統須於上線前進行弱點掃描及滲透測試，且訂定合適的資安檢測週期，並對發現之威脅與弱點採取對應之預防或應變措施。
D10P3 適當情資分享	資通訊系統應建立漏洞揭露和情資分享機制，並確保第三方資安設備漏洞能被及時通知，高風險漏洞應被評估並依計畫可接受方式處理。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	各計畫應就所接受之資安情資，辨識時效性及影響性(比如及時進行威脅與弱點分析以研判潛在風險)，並採取對應之預防或應變措施。
D10P4 設備再重新或汰除前清除資料	系統或設備進行更換、送廠維修或汰除前，應刪除或抹除內容資料，確保資料未經授權的揭露。	● 感知設備 ● IoT 閘道器 ● 網路 ● 後台伺服器 ● 應用程式	系統或設備進行更換、送廠維修或汰除前，應有確保資料安全的處理機制。