CYBERSEC 2021
臺灣資安大會

ORGANIZED BY iThome

TRUST:redefined

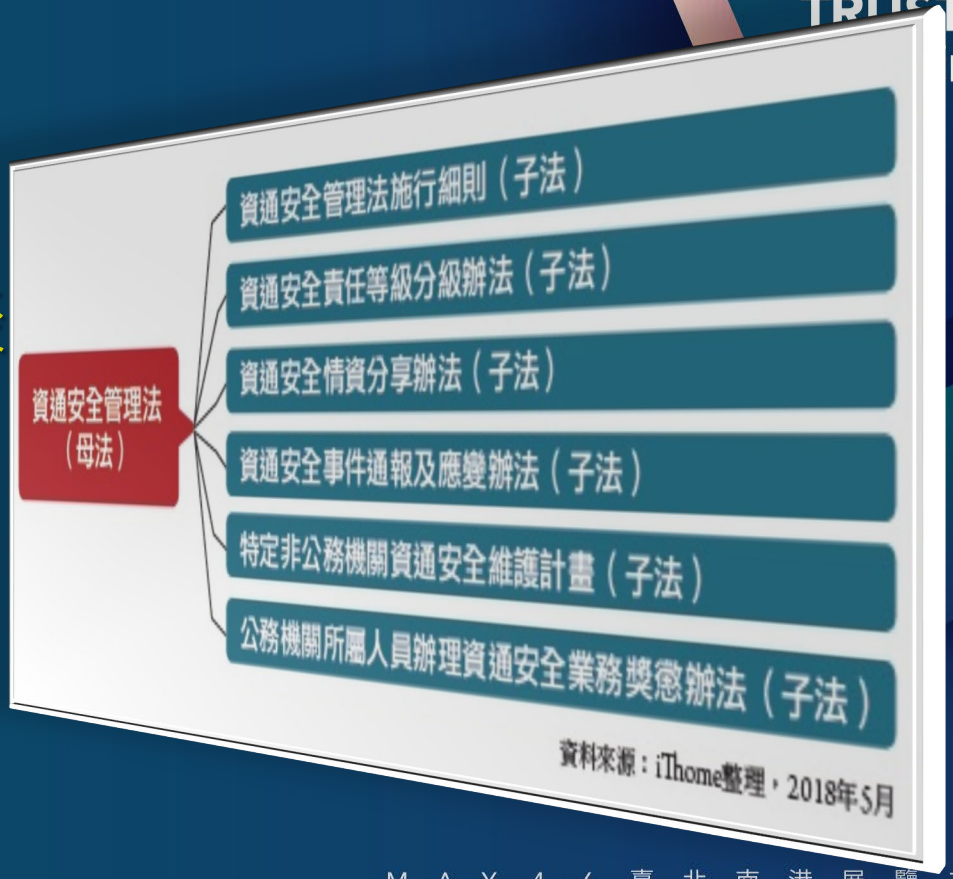
信 任 重 構

醫療資安防護維運經驗談-委外廠商管理經驗分享

七樓701 C會議室

MAY 4-6 臺北南港展覽二館

醫療資安防護維運經驗談
委外廠商管理經驗分享



許世欣 資安長
臺北市立聯合醫院 資通安全管理中心
2021/05/06

法源

- **資通安全管理法 第 9 條**

  公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並**監督**其資通安全維護情形。

- **資通安全管理法施行細則 第4條**

  各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

  一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

  二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

  三、受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

  四、受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

  五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

  六、受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

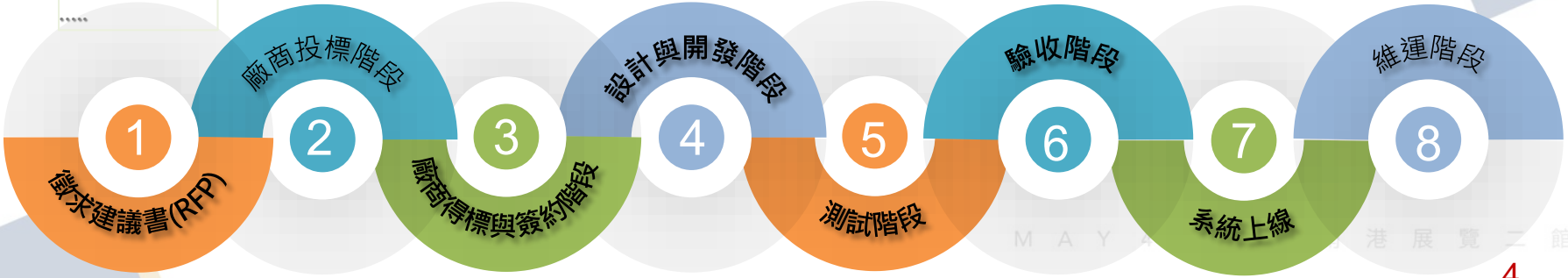
  七、委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

  八、受託者應採取之其他資通安全相關維護措施。

  九、委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

委外服務之各階段管理

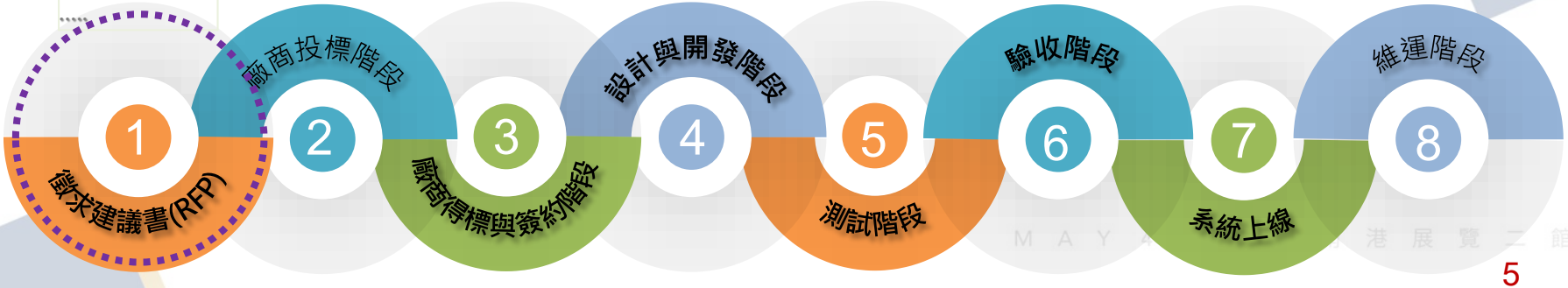
RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	ISMS第三方證書 資安教育證明					
資通安全協議書 二保密切結書 限制使用危害		院資安規範文件 資通安全協議書 廠商保密切結書 成員保密切結書 限制使用危害				
系統防護等級 開發過程規範			SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢			
軟體安全檢測 上線前之檢測 緊急應變計畫 限制使用危害 資安實地訪查 通報應變調查				源碼檢測或弱掃	醫儀資安檢核表 SSDLC-措施驗證 緊急應變計畫	限制使用危害 弱掃滲透鴻碼 維護保養紀錄 資安實地訪查 通報應變調查



委外服務之各階段管理

TRUST: redefined

RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	ISMS第三方證書 資安教育證明	院資安規範文件 資通安全協議書				
資通安全協議書 二保密切結書 限制使用危害		廠商保密切結書 成員保密切結書 限制使用危害				
系統防護等級 開發過程規範			SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢			
軟體安全檢測				源碼檢測或弱掃	醫儀資安檢核表	限制使用危害 弱掃滲透鴻碼 維護保養紀錄 資安實地訪查 通報應變調查
上線前之檢測					SSDLC-措施驗證	
緊急應變計畫						緊急應變計畫
限制使用危害 資安實地訪查 通報應變調查 ……						



RFP資通安全要求 (摘要說明)

一. 等級：院方核定資安防護等級
二. 廠商：資安完備或通過ISO27001驗證
三. 人員：適當之資安訓練（證照或證明）
四. 保密：廠商版及個人版
五. 廠商簽署「委外作業資通安全協議書」
六. 廠商應依SSDLC準則開發及維運
七. 非廠商產品利用之授權證明
八. 不得有後門，有漏洞需配合修補
九. 系統應有防護措施(防毒、防火牆或ACL)
十. 安裝申請、異動申請及組態管理
十一.110/7/1起申請廠商申請VPN資格要求 (通過ISO27001或合格率≧90%)
十二.連線設備須事前經安全檢測
十三.應用系統上版前源碼檢測需無中高風險項
十四.Log留存6個月以上
十五.規劃系統備份及復原演練計畫
十六.接觸之資料不得留存、備份、篡改或販售
十七.事件主動通報、配合應變及事後調查作業
十八.廠商配合本院依法執行開發環境訪查作業
十九.契約終止應歸還本院資產(軟硬體/資料/權限)

專章共3頁

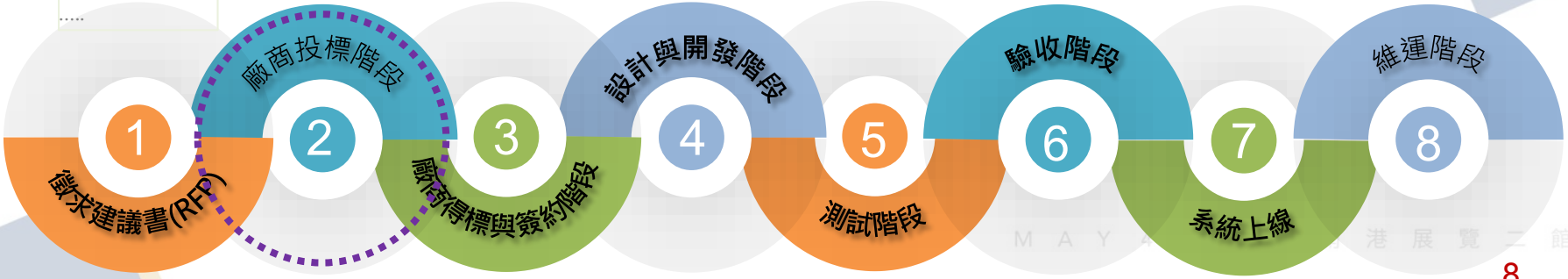
系統防護需求等級

- 依據「資通安全責任等級分級辦法」院方於RFP中標明防護需求等級。
- 本專案之資通系統防護需求等級為「註1」，得標廠商應依「資通安全責任等級分級辦法」附表十資通系統防護基準，規劃、設計及落實執行相關控制措施.....。

註1：普、中、高或*(不適用)

廠商投標階段

RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	**ISMS第三方證書** **資安教育證明**	院資安規範文件 資通安全協議書				
資通安全協議書 二保密切結書 限制使用危害		廠商保密切結書 成員保密切結書 限制使用危害				
系統防護等級 開發過程規範			SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢			
軟體安全檢測 上線前之檢測 緊急應變計畫 限制使用危害 資安實地訪查 通報應變調查				源碼檢測或弱掃	醫儀資安檢核表 SSDLC-措施驗證 緊急應變計畫	限制使用危害 弱掃滲透鴻碼 維護保養紀錄 資安實地訪查 通報應變調查



建議書/規格書資安相關文件

法規要求

資通安全管理法施行細則

- 第4條 第1項：受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證
- 第4條 第2項：受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員

佐證資料

- 資通安全管理措施或通過資通安全第三方驗證（效期內）

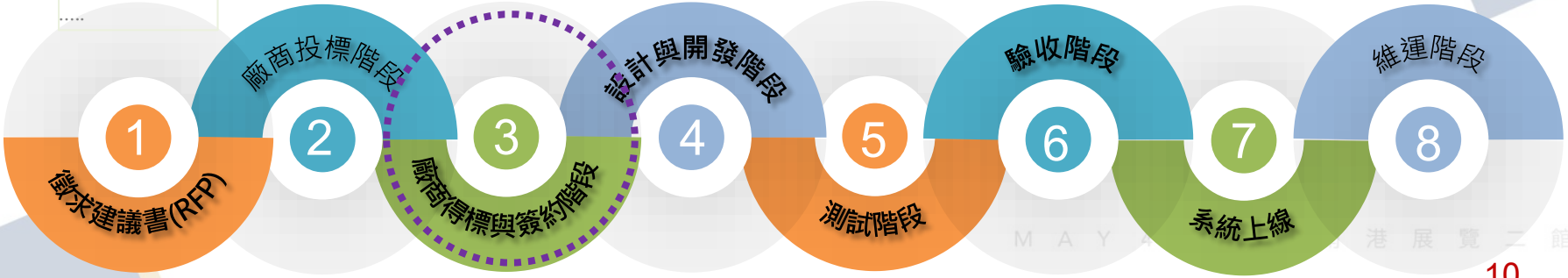
專業證照（請參考行政院國家資通安全會報網站公布之資通安全專業證照列表）

- 專案團隊成員之資安教育訓練資料

廠商得標與簽約階段

TRUST: redefined

RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	ISMS第三方證書 資安教育證明	**院資安規範文件** **資通安全協議書**				
資通安全協議書 二保密切結書 限制使用危害		**廠商保密切結書** **成員保密切結書** **限制使用危害**				
系統防護等級 開發過程規範			SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢			
軟體安全檢測 上線前之檢測 緊急應變計畫 限制使用危害 資安實地訪查 通報應變調查				源碼檢測或弱掃	醫儀資安檢核表 SSDLC-措施驗證 緊急應變計畫	限制使用危害 弱掃滲透鴻碼 維護保養紀錄 資安實地訪查 通報應變調查



廠商簽署契約時資安相關文件

規範要求

- 廠商應瞭解院方之資安規範
- ISMS：A.13.2.4 機密性或保密協議
  依資通安全管理法及本院資安管理規範，得標廠商應簽署「委外廠商執行人員保密切結書」及專案成員應簽署「個人保密切結書」，並確實要求所屬人員遵守保密規定，倘經發現因前述事由而洩密者，一切損害經由得標廠商負責，並依法追究刑事責任。得標廠商成員於受託業務執行期間若有異動，應事先通知本院，並重新簽署保密切結書

繳交資料

- 資通安全協議書
- 公司簽署
  「委外廠商執行人員保密切結書」
- 成員簽署
  「個人保密切結書」
  - 若有異動需事先通知本院

資通安全協議書範例

分資訊、醫儀
版本共42條

委外作業資通安全協議書

立協議書人_____自_____年____月____日起，參與臺北市立聯合醫院(以下簡稱本院)執行【專案名稱　　】，願意配合本院資通安全之運作，執行下列資通安全相關工作：

	資通安全協議項目	本院專案負責人評估是否適用	廠商負責人確認已瞭解配合事項	說明 廠商若無法配合請敘明
一、人力資源管理				
1	廠商專案成員應瞭解資通安全管理法及其子法	□是 □否	□是 □否	
2	廠商應提供專案成員資安專業能力證明文件（如資通安全教育訓練紀錄、資通安全專業證照影本、相關實務經驗佐證等）。	□是 □否	□是 □否	
3	廠商應簽署「委外廠商執行人員保密切結書」。	□是 □否	□是 □否	
4	廠商專案成員應簽署「臺北市立聯合醫院保密切結書」。	□是 □否	□是 □否	
5	廠商專案成員於受託業務執行期間若有異動，應事先通知本院專案負責人，並重新簽署保密切結書。	□是 □否	□是 □否	
6	廠商於契約終止後，依具保密切結要求，對於本院機密業務內容，持續具有保密義務與責任。	□是 □否	□是 □否	
二、存取控制管理				
7	系統管理者權限，於安裝後應交付本院專案負責人，廠商不得私自開設帳號。	□是 □否	□是 □否	

主辦單位
依需求指定

廠商單位
回應或說明

文件編號/名稱	機密等級	生效日	版次	頁次
TpecH-ISMS-4-GE-031 委外作業資通安全協議書	一般	109/06/01	3	1/10

保密切結書

臺北市立聯合醫院委外廠商執行人員保密切結書

立切結書人.....（簽署人姓名）等，受.....（廠商名稱）委派至臺北市立聯合醫院（以下稱本院）處理業務，謹善明恪遵本院下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經本院權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將本院之資訊設備、媒體檔案及公務文書攜出。

二、 未經本院業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接本院網路。若經申請獲准連接本院網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、 經核准攜入之資訊設備欲連接本院網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、 廠商駐點服務及專責維護人員原則應使用本院配發之個人電腦與連通設備，並僅開放使用本院內部網路。若因業務需要使用本院電子郵件、目錄服務，應經本院業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經本院業務相關人員之確認並代為申請核准。

五、 本院得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、 本保密切結書不因立切結書人離職而失效。

七、 立切結書人因違反保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人

姓名及簽章	身分證字號	聯絡電話及戶籍地址

立切結書人所屬廠商：

廠商名稱及蓋章	廠商負責人姓名及簽章	廠商聯絡電話及地址

公司簽署

臺北市立聯合醫院保密切結書

立切結書人_____自民國_____(年月日)起

□擔任臺北市立聯合醫院員工

□受_____(廠商名稱)委派至臺北市立聯合醫院執行_____業務(專案案號及名稱)

□其他_____ 例如：PGY、實習生、見習生、志工、查核委員等(請填載業務內容)

對於業務上所持有、知悉或偶然得知或偶然持有之臺北市立聯合醫院病人之病情、健康資訊、隱私、公務機密或敏感性資訊、程式及其檔案、媒體、院內網頁內容等，願善盡保管及保密之責，不得以口頭、複印、借閱、交付、文章發表、電子郵件、透過網路或他法，散佈或洩漏予其他第三人，並遵守國家機密保護法、個人資料保護法、資通安全管理法、醫療法、電子簽章法、著作權法及檔案法等相關法規以及臺北市立聯合醫院各項公務機密處理規定，保密義務與責任不因立切結書人離職或所執行之專案業務結束而失效。如有違誤，願賠償一切因此所生之損害及相關法律責任。

立切結書人同意本切結書利用電子簽章或電子文件方式交換之電子訊息，其效力與書面簽署或書面文件相同。

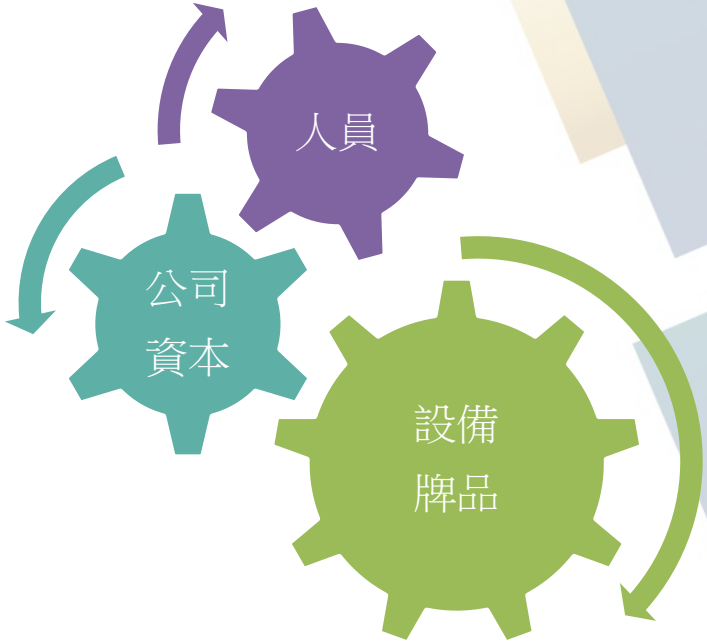
個人簽署

限制使用危害國家資通安全產品

一、除因業務需求且無其他替代方案外，不得採購及使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。

二、必須採購或使用危害國家資通安全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置。

三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應列冊管理，且不得與公務網路環境介接。



設計與開發階段

RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	ISMS第三方證書 資安教育證明	院資安規範文件 資通安全協議書				
資通安全協議書 二保密切結書 限制使用危害		廠商保密切結書 成員保密切結書 限制使用危害				
系統防護等級 開發過程規範			**SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢**			
軟體安全檢測 上線前之檢測 緊急應變計畫 限制使用危害 資安實地訪查 通報應變調查				源碼檢測或弱掃	醫儀資安檢核表 SSDLC-措施驗證 緊急應變計畫	限制使用危害 弱掃滲透鴻碼 維護保養紀錄 資安實地訪查 通報應變調查

設計與開發階段繳交資安相關文件

法規要求

- 資通安全責任等級分級辦法 第11條 各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施。
  - 普：31項； 中：56項； 高：76項
- 資通安全管理法施行細則第4條第5款.....涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

繳交資料

- TpecH-ISMS-4-GE-030SSDLC採取措施及驗證查核表
  (於系統設計階段，填具採取措施)
- 若有：需提供軟體授權證明

SSDLC(附表十)Excel表格

	A	B	C	D	E	F	G	H	I	J	K
1		系統名稱				機密性					
2						完整性：					
3		功能說明：				可用性：					
4						法遵性：					
5		業務單位：				防護需求等級：					
6	序號	構面	控制措施	安全需求項目	說明	本院規範	普	中	高	類別	採取措施
7	1	存取控制	帳號管理	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序	資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、開通、停用或刪除之行為。	TpecH-ISMS-2-GE-003 資通安全存取控制	普	中	高	技術	
8	2			已逾期之臨時或緊急帳號應刪除或禁用	若具有臨時帳號或緊急帳號時，應實作已逾期之系統帳號檢查機制，於帳號逾期時自動停用或刪除，以避免帳號遭有心人士盜用。	TpecH-ISMS-2-GE-003 資通安全存取控制		中	高	技術	
9	3			資通系統閒置帳號應禁用	宜記錄系統帳號最後登入時間，可透過工作排程，檢查是否有持續一段時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。	TpecH-ISMS-2-GE-003 資通安全存取控制		中	高	技術	
10	4			定期審核資通系統帳號之建立、修改、啟用、盤點、禁用及刪除	定期審核資通系統帳號使用現況，檢視是否存在帳號被異常建立、竄改或啟用等行為，並禁用或刪除閒置帳號與臨時帳號。	TpecH-ISMS-2-GE-003 資通安全存取控制		中	高	維運	
11	5			逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出	會談(Session)機制目的為管理使用者與伺服器之間的連線狀態，使用者於系統中若一段時間(15分鐘)未進行活動，系統應有自動機制將該使用者的會談階段設為失效而登出系統，以降低資安風險。	TpecH-ISMS-2-GE-003 資通安全存取控制			高	技術	
12	6			應依機關規定之情況及條件，使用資通系統	應依據機關規定之情況及條件(如特定時間或指定IP來源等)，限制系統使用行為(如僅開放平時上班時間使用系統、特定功能或機敏資訊僅允許透過內部網路存取等)。	TpecH-ISMS-2-GE-003 資通安全存取控制			高	技術	
13	7			監控資通系統帳號，如發現帳號違常使用時回報管理者	應具備監控及通知機制，向系統管理者回報帳號異常使用行為(如短期內大量帳號登入失敗或存取未經授權之資源等)。	TpecH-ISMS-2-GE-003 資通安全存取控制			高	技術	

工作表2

SSDLC(附表十)管理軟體

ISMS04[防護基準管理(另稱SSDLC)][院本部]

作業模式　檢視畫面

維護(F3)　查詢(F5)　進階查詢

盤點年度 109　資產名稱 資通安

擁有院區　部門

管理院區　部門

複製	完成比例	年度
	31/31	109

資產名稱 資通安全管理系統

系統屬性 行政　版本類別

含機敏資料 N　機密性 1

防護需求等級 普　導入ISMS N

符合防護基準 符合　不符合

執行查詢(Q) F5　總計1筆　許世欣　110/05/03 17:02

ISMS04[防護基準管理(另稱SSDLC)][院本部]

作業模式　檢視畫面

防護基準採取措施表

綠底白色字表示已完成填寫，淺綠底紅色字表示完成一項填寫，白底黑字表示尚未填寫

年度	序號	控制措施名稱	控制措施內容	控制措施說明	採取措施
109	1	帳號管理	建立帳號管理機制，包含帳號之申請、開通、...	資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使...	依據TpecH-ISMS-
109	9	遠端存取	對於每一種允許之遠端存取類型，均應先取得...	機關應明確訂定資通系統之存取限制、組態需求、連線需求，並將這些資訊文...	依據TpecH-ISMS-
109	13	稽核事件	依規定時間週期及紀錄留存政策()，保留稽核...	應依機關規定之時間週期及紀錄留存政策(至少3個月)，保留系統稽核(指日誌)...	依據TpecH-ISMS-
109	14	稽核事件	確保資通系統有稽核特定事件之功能，並決定...	資通系統應實作稽核(指日誌)特定事件之功能，如身分驗證失敗、存取資源失...	針對帳號登入、密
109	15	稽核事件	應稽核資通系統管理者帳號所執行之各項功能	系統管理者為資通系統內具有最高權限之帳號，對系統及資料極具影響力，記...	針對帳號登入、密
109	17	稽核紀錄內容	資通系統產生之稽核紀錄應包含事件類型、發...	稽核(指日誌)紀錄應詳細描述所觸發的事件，包含人、事、時、地、物等關鍵...	透過Guardian記錄
109	19	稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之...	資通系統應配置稽核(指日誌)紀錄所需之儲存容量(如磁碟或資料庫空間等)，避...	系統組依據程式人
109	20	稽核處理失效之回應	資通系統應在稽核處理失效時，應採取適當之...	稽核(指日誌)處理失效時，應訂定相對應的處理措施(如覆寫最舊的稽核(指日誌)...	系統組定期監控日
109	22	時戳及校時	資通系統應使用系統內部時鐘產生稽核紀錄所...	使用系統內部時鐘(本院之鐘訊主機)產生稽核紀錄所需時戳，採用全系統一致...	採用NTP校時機制

控制措施　建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序

控制說明　資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、開通、停用或刪除之行為。

查詢本院規範　TpecH-ISMS-2-GE-003資通安全存取控制

採取措施　依據TpecH-ISMS-2-GE-003資通安全存取控制程序書，已建置程序。
1. 系統與資料應依使用者角色，設計存取功能及範圍，並填具「TpecH-ISMS-4-GE-023 資通系統角色對應表」。
2. 帳號權限申請表：帳號申請之表單為「TpecH-ISMS-4-GE-024 資通系統帳號權限申請單(IT)」。

驗證結果 Y

後續驗證方式　程序已建置

取消

存檔

防護基準採取措施表

設計與開發階段相關活動之資安要求

規範要求

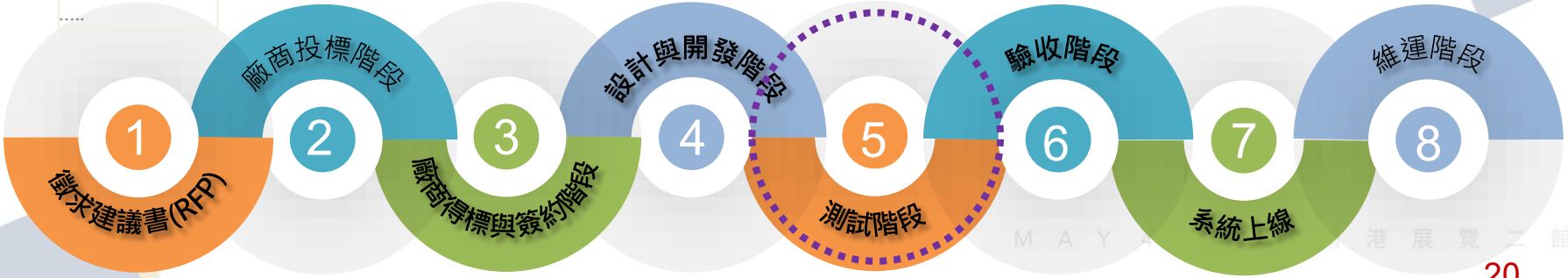
- ISMS：A.6.2.行動裝置及遠距工作
  - VPN網路連線申請單
  - 通信安全應採取網路通訊加密機制
  - 裝置於輸入、輸出資料前後，必須以手動方式進行掃毒，始得以連接
- ISMS：A.12.1運作程序及責任
  - 變更管理
  - 容量管理
  - 開發、測試及運作環境之區隔

配合事項

- 遠距工作
  - VPN網路連線申請單
  - (110年7月起通過ISO驗證或查核合格者始得申請)
  - 人員異動必須事先通知本院
- 連線設備需先完成掃毒檢測
- 實際作業
  - 「TpecH-ISMS-4-GE-039資通設備系統安裝／維護紀錄單」(IT)
  - 「TpecH-ISMS-4-GE-052新購醫療儀器設備資通安全檢核表」(OT)
  - 不得於正式環境進行測試作業

測試階段

RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	ISMS第三方證書 資安教育證明	院資安規範文件 資通安全協議書				
資通安全協議書 二保密切結書 限制使用危害		廠商保密切結書 成員保密切結書 限制使用危害				
系統防護等級 開發過程規範			SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢			
軟體安全檢測 上線前之檢測 緊急應變計畫 限制使用危害 資安實地訪查 通報應變調查				**源碼檢測或弱掃**	醫儀資安檢核表 SSDLC-措施驗證 緊急應變計畫	限制使用危害 弱掃滲透鴻碼 維護保養紀錄 資安實地訪查 通報應變調查



測試階段之資安要求

法規要求

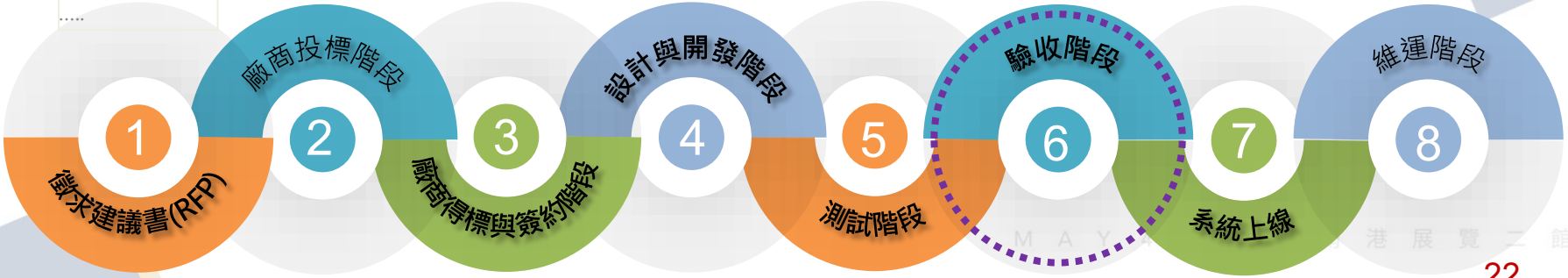
- 資通安全管理法施行細則 第5條 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測

配合事項

- 於上線測試前廠商能提供
  - 弱點掃描
  - 分級「高」者要有
    - 滲透測試、源碼檢測
- 金額超過新臺幣一千萬元以上者，院方另進行安全性檢測

驗收階段

RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	ISMS第三方證書 資安教育證明					
資通安全協議書 二保密切結書 限制使用危害		院資安規範文件 資通安全協議書 廠商保密切結書 成員保密切結書 限制使用危害				
系統防護等級 開發過程規範			SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢			
軟體安全檢測 上線前之檢測 緊急應變計畫 限制使用危害 資安實地訪查 通報應變調查				源碼檢測或弱掃	**醫儀資安檢核表** **SSDLC-措施驗證**	緊急應變計畫	限制使用危害 弱掃滲透鴻碼 維護保養紀錄 資安實地訪查 通報應變調查



驗收階段之資安要求

規範要求

- 資通安全責任等級分級辦法 第11條
  各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施。
  - 普：31項； 中：56項； 高：76項
- 資通安全管理法施行細則第4條第5項.....涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

繳交資料

- TpecH-ISMS-4-GE-030SSDLC 採取措施及驗證查核表
  (於驗證階段，進行措施驗證)
- 若有：需提供軟體授權證明

SSDLC(附表十) Excel表格

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	序號	構面	控制措施	安全需求項目	說明	本院規範	普	中	高	類別	採取措施	驗證方式	驗證結果
2	1	存取控制	帳號管理	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序	資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、開通、停用或刪除之行為。	TpecH-ISMS-2-GE-003資通安全存取控制	普	中	高	技術			
3	2			已逾期之臨時或緊急帳號應刪除或禁用	若具有臨時帳號或緊急帳號時，應實作已逾期之系統帳號檢查機制，於帳號逾期時自動停用或刪除，以避免帳號遭有心人士盜用。	TpecH-ISMS-2-GE-003資通安全存取控制		中	高	技術			
4	3			資通系統閒置帳號應禁用	宜記錄系統帳號最後登入時間，可透過工作排程，檢查是否有持續一段時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。	TpecH-ISMS-2-GE-003資通安全存取控制		中	高	技術			
5	4			定期審核資通系統帳號之建立、修改、啟用、盤點、禁用及刪除	定期審核資通系統帳號使用現況，檢視是否存在帳號被異常建立、竄改或啟用等行為，並禁用或刪除閒置帳號與臨時帳號。	TpecH-ISMS-2-GE-003資通安全存取控制		中	高	維運			
6	5			逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出	會談(Session)機制目的為管理使用者與伺服器之間的連線狀態，使用者於系統中若一段時間(15分鐘)未進行活動，系統應有自動機制將該使用者的會談階段設為失效而登出系統，以降低資安風險。	TpecH-ISMS-2-GE-003資通安全存取控制			高	技術			
7	6			應依機關規定之情況及條件，使用資通系統	應依據機關規定之情況及條件(如特定時間或指定IP來源等)，限制系統使用行為(如僅開放平時上班時間使用系統、特定功能或機敏資訊僅允許透過內部網路存取等)。	TpecH-ISMS-2-GE-003資通安全存取控制			高	技術			
					應具備監控及通知機制，向系統管理者回								

工作表2

TRUST : redefined

資通設備系統安裝/維護紀錄單

□安裝, □維護, □POC

設備名稱：

設備位置： 位置描述（_____院區 _____機房(空間)_____機櫃）

由_____ 入_____

申請日時分：

委外廠商： 委外人員：

依據：

申請原因 [*或附變機說*]

變更影響評估

- 影響備份或回復計畫？ □是, □否
- 完成事前備份？ □是, □否
- 組態開異動 □是, □否
- 影響範圍（關聯應用系統）：

申請審核					
經辦人員		主管		會辦單位	

文件編號/名稱	機密等級	生效日	版次	頁次
TpecH-ISMS-4-GE-039 資通設備系統安裝/維護紀錄單	一般	109/06/1	3	1/2

資安封面表單

合約案號

	查驗內容(廠商填)	查驗結果(院方填)	
資訊中心審查之繳交文件	(1) 本儀器具備資通訊能力或設備? □是, □否(以下 2~9 選項免填)		
	(2) 網路架構圖	□已繳	□免繳
	(3) 是否有對外傳輸功能 □網路孔, □Wi-Fi, □USB 孔, □RS232, □藍芽, □其他___	□有	□無
	(4) 連網路□無,□有 IP_____(納入醫院 AD 管理：□有, □無)	□有風險	□無風險
	(5) 啟連線設備 IP(Port)：		
	(6) 安裝防毒軟體(_____)至病毒碼版本(_____)證明	□有風險	□無風險
	(7) 醫療儀器電腦之作業系統版本_____	□有風險	□無風險
	(8) 設小型防火牆以防護(3)~(6)項之風險? □有， □無	□有防護	□無防護
	(9) 醫療儀器設備(含周邊)系統，是最新修補日期_____	□是	□否
	(10)是否對院外傳輸資料?	□是	□否
	(11) 原廠維護手冊(1 份)	□已繳	□免繳
醫工室審查之繳交文件	(12) □中文操作手冊(2 份)；□中文簡易操作卡及故障排除卡	□已繳	□免繳
	(13) 中文簡易故障排除卡	□已繳	□免繳
	(14) 教育訓練簡報	□已繳	□免繳
	(15) 器械項目廠商需列表造冊（含）器械照片之電子檔	□已繳	□免繳
	(16) 醫療儀器需提供貴重零件(十萬元以上)價格對照表	□已繳	□免繳
	(17) 耗材價格表,如壓脈帶、ECG 導線、SpO2 感測線等相關耗材	□已繳	□免繳
	(18)儀器設定資訊(組態設定) (□電子檔， □紙本文件)	□已繳	□免繳
	(19)電性安全(須附*出廠測試報告*，於測試報告中明確標註出以下數值，並附上原廠規範之安全範圍)		
	①電源供應 ___ A ___V (標準值：__A___V)	□合格	□免測
	②接地電阻：_____Ω (<0.15Ω)	□合格	□免測
	③機殼漏電電流：_____μA (<300μA), 未接觸病患<500μA	□合格	□免測

本份資料繳交至醫工室

廠商聲明： 廠商大小印

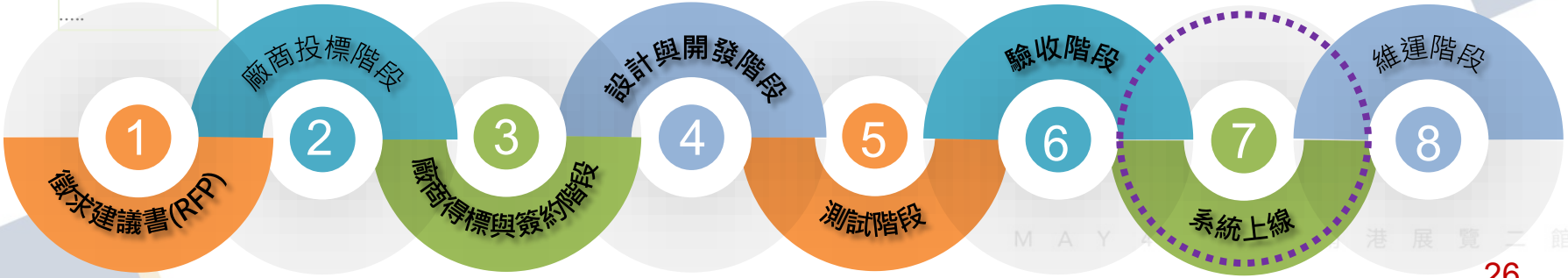
本公司於臺北市立聯合醫院之本案交機設備
均符合醫院訂定之「資通安全管理規範」規定。

文件編號/名稱	機密等級	生效日	版次	頁次
TpecH-ISMS-4-GE-052 新購醫療儀器設備資通安全檢核表	一般	109/06/01	1	2/2

新購醫療儀器設備資通安全檢核表

系統上線

RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	ISMS第三方證書 資安教育證明					
資通安全協議書 二保密切結書 限制使用危害		院資安規範文件 資通安全協議書 廠商保密切結書 成員保密切結書 限制使用危害				
系統防護等級 開發過程規範			SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢			
軟體安全檢測 上線前之檢測 緊急應變計畫 限制使用危害 資安實地訪查 通報應變調查				源碼檢測或弱掃	醫儀資安檢核表 SSDLC-措施驗證	緊急應變計畫	限制使用危害 弱掃滲透鴻碼 維護保養紀錄 資安實地訪查 通報應變調查



系統上線之資安文件

法規要求

- ISMS：A.16.1.5對資訊安全事故之回應

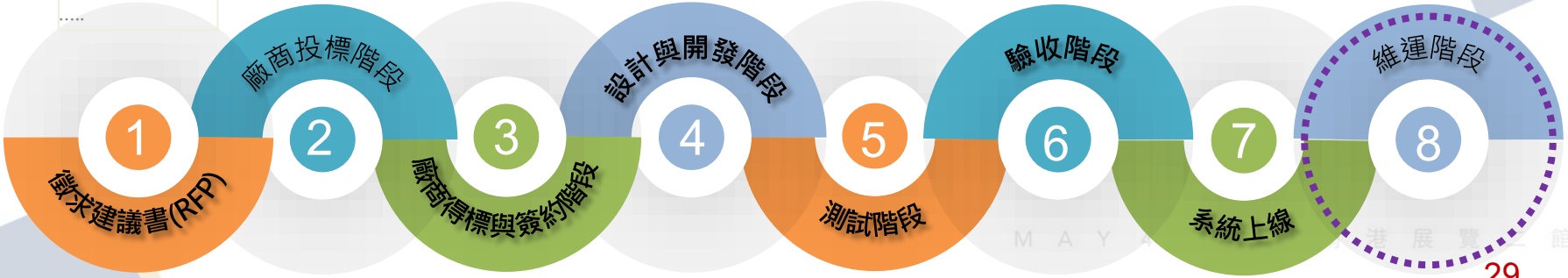
繳交資料

- 廠商對所承攬之系統撰寫緊急應變計畫，內容含括:
  - 預防作業
  - 整備作業
  - 應變作業(可依情境條述)
  - 復原作業

緊急應變計畫範例

維運階段

RFP資安要求	廠商建議書	簽署契約				
資安相關證照 資安相關證明	ISMS第三方證書 資安教育證明					
資通安全協議書 二保密切結書 限制使用危害		院資安規範文件 資通安全協議書 廠商保密切結書 成員保密切結書 限制使用危害				
系統防護等級 開發過程規範			SSDLC-採行措施 他軟體授權證明 組態申請及安裝 連線設備之安檢			
軟體安全檢測 上線前之檢測 緊急應變計畫 限制使用危害 資安實地訪查 通報應變調查				源碼檢測或弱掃	醫儀資安檢核表 SSDLC-措施驗證 緊急應變計畫	**限制使用危害** **弱掃滲透鴻碼** **維護保養紀錄** **資安實地訪查** **通報應變調查**



資通設備系統安裝/維護紀錄單

☐安裝, ☐維護, ☐POC

設備名稱：	
設備位置： 位置描述（_____院區 _____機房(空間)_____機櫃） 由_____ 入_____	
申請日時分：	
委外廠商：	委外人員：
依據：	
申請原因 [如問題概述]	

變更影響評估

- 影響備份或回復計畫？ ☐是, ☐否
- 完成事前備份？ ☐是, ☐否
- 組態異動 ☐是, ☐否
- 影響範圍（關聯應用系統）：

申請審核

經辦人員		主管		會辦單位	

文件編號/名稱	機密等級	生效日	版次	頁次
TpecH-ISMS-4-GE-039 資通設備系統安裝/維護紀錄單	一般	109/06/1	3	1/2

資安封面表單

委外廠商：	
委外人員：	執行日期：
原因分析	
處理經過	
測試結果	
資安檢核	本儀器具備資通訊能力或設備? ☐是, ☐否(以下選項免填)
	第 1 節：☐本節相關資訊同安裝時註記，☐本節有異動如下
	是否使用以下接口對外傳輸功能：☐無 ☐網路孔, ☐Wi-Fi, ☐USB 孔, ☐RS232, ☐藍芽, ☐其他____
	(1) 連網路☐無, ☐有 IP_____(納入醫院 AD 管理：☐有, ☐無) 欲連線設備 IP(Port)：
	安裝防毒軟體(_____)至病毒碼版本(_____)證明，
	醫療儀器電腦之作業系統版本_____
	設小型防火牆以防護(1)~(4)項之風險? ☐有， ☐無
	醫療儀器設備(含周邊)系統，最新修補日期_____
	是否對院外傳輸資料? ☐是， ☐否
	第 2 節：容量管理、組態管理及校時管理
	A. 容量管理：剩餘儲存空間 %
	B. 儀器設定資訊：組態設定 ☐電子檔，☐紙本文件
	C. 時間校正方式 ☐鐘訊校時， ☐手動校時

結果確認

使用單位		醫工單位	

文件編號/名稱	機密等級	生效日	版次	頁次
TpecH-ISMS-4-GE-051 醫儀設備系統維護紀錄單	一般	110/01/01	4	2/2

醫儀設備系統維護紀錄單

維運階段之資安活動(1)

法規要求

- A.16.1.3事件或弱點之通報要求
- 資通安全事件通報及應變辦法
- 機關應辦事項
  - 安全性檢測

繳交資料

- 事件通報內容
  - 通報者之單位及姓名
  - 事件發生地點或部門
  - 事件發生或知悉時間
  - 事件狀況之描述
- 配合應變演練
- 配合事件調查報告
  - 於事件後發生15日內提報給對口單位
- 安全性檢測之修補

維運階段之資安活動(2)

法規要求

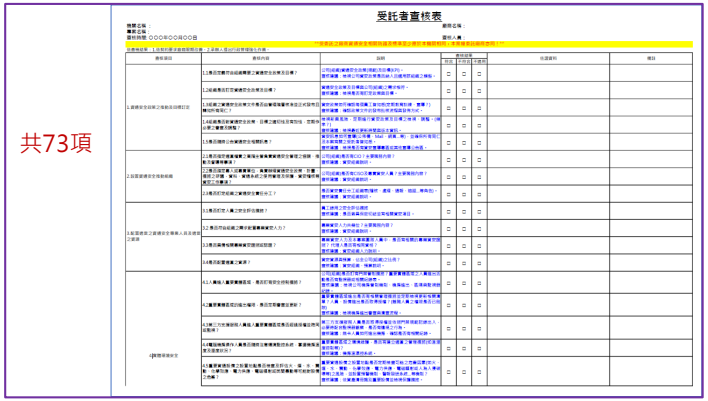
- 資通安全管理法施行細則 第4條第九項

  委託機關應**定期**或於知悉受託者發生**可能影響**受託業務之資通安全事件時，以**稽核**或其他適當方式確認受託業務之執行情形。

- 台北市政府查核SOP
  - 受託者查核項目表

配合事項

- 準備受稽文件
- 擇定受稽日(1日)
- 受稽日之人力配合
- 針對缺失進行改善



共73項

受託者查核表

機關名稱：
專案名稱：
查核時間: ○○○年○○月○○日

廠商名稱：
查核人員：

受委託之廠商資通安全相關防護及標準至少應於本機關相同，本案複委託廠商亦同！

依查核結果：1.依契約要求廠商限期改善。2.承辦人提出行政管理強化作業。

查核項目	查核內容	說明	查核結果			佐證資料	備註
			符合	不符合	不適用		
1.資通安全政策之推動及目標訂定	1.1是否定義符合組織需要之資通安全政策及目標？	公司(組織)資通安全政策(規範)及目標(KPI)。 查核建議：檢視公司資安政策是否納入且適用該組織之類型。	□	□	□		
	1.2組織是否訂定資通安全政策及目標？	資通安全政策及目標與公司(組織)之需求相符。 查核建議：檢視是否有訂定政策與目標。	□	□	□		
	1.3組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	資安政策如何確認每個員工皆知悉(定期教育訓練、宣導？) 查核建議：確認政策文件的發布批核流程與發佈方式。	□	□	□		
	1.4組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	檢視新興風險，定期進行資安政策及目標之檢視、調整。(頻率？) 查核建議：檢視最近更新時間與版本資訊。	□	□	□		
	1.5是否隨時公告資通安全相關訊息？	資安訊息如何宣導(公佈欄、Mail、網頁...等)，並確保所有同仁及本案有關之受託者皆知悉。 查核建議：檢視是否有資安宣導專區或其他宣導公告區。	□	□	□		
2.設置資通安全推動組織	2.1是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	公司(組織)是否有CIO？主要職務內容？ 查核建議：資安組織說明。	□	□	□		
	2.2是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	公司(組織)是否有CISO及專責資安人員？主要職務內容？ 查核建議：資安組織說明。	□	□	□		
	2.3是否訂定組織之資通安全責任分工？	是否資安責任分工組織表(稽核、處理、通報、追蹤...等角色)。 查核建議：資安組織說明。	□	□	□		
3.配置適當之資通安全專業人員及適當之資源	3.1是否訂定人員之安全評估措施？	員工錄用之安全評估措施 查核建議：是否簽具保密切結並有相關資安項目。	□	□	□		
	3.2 是否符合組織之需求配置專業資安人力？	專職資安人力共幾位？主要職務內容？ 查核建議：資安組織說明。	□	□	□		
	3.3是否具備相關專業資安證照或認證？	專職資安人力及本專案團隊人員中，是否有相關的專業資安證照？代理人是否有相同資格？ 查核建議：資安組織人力說明。	□	□	□		
	3.4是否配置適當之資源？	資安資源與預算，佔全公司(組織)之比例？ 查核建議：資安組織、預算說明。	□	□	□		
4.實體環境安全	4.1人員進入重要實體區域，是否訂有安全控制措施？	公司(組織)是否訂有門禁管制措施？重要實體區域之人員進出活動是否有監視器或相關紀錄表。 查核建議：檢視公司機房管制機制、機房進出、區隔與監視器紀錄。	□	□	□		
	4.2重要實體區域的進出權限，是否定期審查並更新？	重要實體區域進出是否有相關管理措施並定期檢視更新相關清單？人員、設備進出是否取得授權？(離職人員之權限是否已刪除) 查核建議：檢視機房進出審查與清查流程。	□	□	□		
	4.3第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	第三方支援服務人員是否取得授權並依照門禁規範記錄出入，必要時配合監視器觀察，是否有違規之行為。 查核建議：無卡人員如何進出機房，確認是否有相關紀錄。	□	□	□		
	4.4電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及濕度狀況？	重要實體區域之環境維護，是否有建立適當之管理措施(如溫濕度控制等)？ 查核建議：機房溫濕控系統。	□	□	□		
	4.5重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁輻射或民間暴動等可能對設備之危害？	重要資通設備之設置地點是否定期檢查可能之危害因素(如火、煙、水、震動、化學效應、電力供應、電磁輻射或人為入侵破壞等)之風險，並設置預警機制、警報發送系統...等機制？ 查核建議：依資產清冊識別重要設備並檢視保護措施。	□	□	□		

契約終止時之資安活動

法規要求

- 資通安全管理法施行細則 第4條
  - 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

配合事項

- 返還文件
- 移交文件
- 移出設備或報廢(若有)
  - 儲存媒體抹除後始得移出

謝謝您的聆聽