

附錄一 公文電子交換系統資訊安全自評表

編號	檢核項目		自評結果	相關佐證說明
1	管 ¹	程式之開發設計應納入密碼原則、資料有效性檢核及資料加密防護等安全性考量，並確保未被植入惡意程式。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
2	管	定期審視作業系統漏洞修補訊息，評估作業系統變更對本系統運作及安全產生之影響，並依據評估及測試結果，對本系統做必要調整，再進行作業系統變更，並對交換層發布作業系統更新通知。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交	配合管理層發布之作業系統更新及漏洞修補通知，於一週內排定更新時程並儘速完成更新。		
3	管	建立本系統程式版本控制及安全更版機制，更版之版本應以憑證簽章，確保更版過程未經竄改。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交	於接獲本系統更版通知後，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。		
4	管	針對交換層及機關層主機作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組態設定等作為系統安全維護設定之準則。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交	依循作業環境標準組態列表進行設定。		
5	管	本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，非必要應禁止與網際網路進行連線。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
6	管	配合各交換層主機 IP 位址之變動，更新交換主機 IP 位址清單，並據以修正防火牆白名單設定，同時通知各交換層機關。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交	依據管理層通知之交換主機 IP 位址清單進行防火牆白名單設定，如有交換主機 IP 位址異動需求，應通知管理層辦理連線異動事宜。		
7	交	交換層機關應以防火牆白名單控管機關層及網頁版公文收發模組用戶連線作業，並以一對一固定 IP 位址為原則，如機關層及網頁版公文收發模組用戶有 IP 位址異動需求，應通知交換層辦理連線異動事宜；確有一對多或非固定 IP 位址之需求者，應向交換層機關申請核准，並應建立 IP 位址與機關(構)名稱對照表，以供追蹤及查檢之用。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
8	管	具有防範公文電子交換主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
9	管	主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			

¹以「管」、「交」分別標記為管理層及交換層之檢核項目

編號	檢核項目		自評結果	相關佐證說明
10	管	當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並暫停相關主機服務，避免惡意程式蔓延，並追查惡意程式來源，通知來源機關(構)儘速處理惡意程式。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
11	管	訂定本系統安全傳輸協定，確保傳遞過程全程加密，並建立收發文確認機制，防止未經授權之資料存取及竄改。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
12	管	定期進行本系統網頁及主機弱點掃描，並就掃描結果予以修補，且同時更新交換層及機關層相關程式。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交	定期進行本系統之網頁及主機弱點掃描，並將掃描結果提供管理層研析。		
13	管	定期辦理原碼檢測及滲透測試，或定期辦理資訊安全健檢，並進行必要之修補作業，以預防或發現未知之威脅或攻擊。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
14	管	系統開發與維運工程師每年至少接受六小時安全程式撰寫技術及駭客攻擊手法攻防等資訊安全課程。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
15	管	應檢查主機安裝之伺服器應用軟體憑證效期，並於憑證效期過期前更新憑證，避免交換異常。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
16	管	每年辦理之公文電子交換系統管理維護教育訓練應包含資訊安全(含個人資料保護)議題。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
17	管	應將公文電子交換系統納入 ISMS 第三方認證範圍與資安監控中心(SOC)監控範圍防護，SOC 監控範圍須包含主機及應用系統日誌(log)監控。 自管中心須將日誌傳送至管理層進行監控聯防，如自管中心為實體隔離環境，則須依管理層提供之監控規則進行布署設定。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
18	管	應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
19	管	主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
20	管	應使用並妥善保管管理層發交之密碼模組 I 辦理公文電子交換作業。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			

編號	檢核項目		自評結果	相關佐證說明
21	管	本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
22	管	至少應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理本系統維護作業，委外作業應依資通安全管理法施行細則第四條規定辦理。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	交			
23	交	交換層機關提供網頁版公文收發模組介接使用本系統，應依本規範之要求辦理管理作業。	<input type="checkbox"/> 符合 <input type="checkbox"/> 部分符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		總結：		

自評機關：			
承辦人：	聯絡電話：	email:	
單位主管：	聯絡電話：	email:	
填表日期：			