

項目	(七) 資通安全防護及控制措施				
7.1	<p>是否依法規定期辦理安全性檢測及資通安全健診？</p> <p>1.全部核心資通系統辦理弱點掃描（A 級機關：每年 2 次；B 級機關：每年 1 次；C 級機關：每 2 年 1 次）</p> <p>2.全部核心資通系統辦理滲透測試（A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次）</p> <p>3.資通安全健診，包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆設定檢視等？（A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次）</p>				
7.2	<p>是否針對安全性檢測及資通安全健診結果執行修補作業，且於修補完成後驗證是否完成改善？</p>				
7.3	<p>【A、B 級機關適用】</p> <p>是否完成政府組態基準導入作業？</p> <p>【不適用特定非公務機關】</p>				
7.4	<p>【A、B 級公務機關應於 111 年 8 月 24 日前或核定後 1 年內完成；C 級公務機關應於 112 年 8 月 24 日前或核定後 2 年內完成】是否完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定方式提交資訊資產盤點資料？是否針對高風險弱點進行修補或執行其他控制措施？</p> <p>【特定非公務機關：A、B、C 級關鍵基礎設施提供者】</p>				
7.5	<p>【A、B 級公務機關應於 112 年 8 月 24 日前或核定後 2 年內完成】是否完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定方式提交偵測資料？是否偵測異常事件判定為資安事件後有回傳相關資料？</p> <p>【不適用特定非公務機關】</p>				
7.6	是否完成下列資通安全防護措施？				
	安全防護項目	A 級	B 級	C 級	D 級
	防毒軟體	√	√	√	√
	網路防火牆	√	√	√	√
	電子郵件過濾機制	√	√	√	
	入侵偵測及防禦機制	√	√		
	應用程式防火牆 (具有對外服務之核心資通系統者)	√	√		

	進階持續性威脅攻擊防禦	v			
7.7	是否 <b>針對</b> 電子郵件進行過濾，且 <b>定期</b> 檢討及更新郵件過濾規則？是否 <b>針對</b> 電子郵件 <b>進行</b> 分析，主動 <b>發現</b> 異常行為且進行改善（如針對大量異常電子郵件來源之 IP 位址，於防火牆進行阻擋等）？是否有電子郵件之 <b>使用</b> 管控措施，且落實執行？是否依郵件內容之機密性、敏感性規範傳送 <b>限制</b> ？				
7.8	是否 <b>建立</b> 電子資料安全管理機制，包含分級規則（如機密性、敏感性、一般性等）、存取權限、資料安全、人員管理及處理規範等，且 <b>落實</b> 執行？				
7.9	是否 <b>建立</b> 網路服務安全控制措施，且 <b>定期</b> 檢討？是否 <b>定期</b> 檢測網路運作環境之安全漏洞？				
7.10	是否已確實 <b>設定</b> 防火牆並 <b>定期</b> 檢視防火牆規則，DNS 查詢是否僅限於 <b>指定</b> DNS 伺服器？ <b>有效</b> 掌握與管理防火牆連線部署？				
7.11	針對機關內部同仁及委外廠商 <b>進行</b> 遠端維護資通系統，是否採「原則禁止、例外允許」方式辦理，並有 <b>適當</b> 之防護措施？				
7.12	網路架構設計是否 <b>符合</b> 業務需要及資安要求？是否依網路服務需要 <b>區隔</b> 獨立的邏輯網域（如 DMZ、內部或外部網路等），且 <b>建立</b> 適當之防護措施，以 <b>管制</b> 過濾網域間之資料存取？				
7.13	是否 <b>針對</b> 機關內無線網路服務之存取及應用 <b>訂定</b> 安全管控程序，且 <b>落實</b> 執行？				
7.14	資通系統重要組態設定檔案及其他具保護需求之資訊是否 <b>加密</b> 或其他適當方式 <b>儲存</b> （如實體隔離、專用電腦作業環境、資料加密等）？是否 <b>針對</b> 資訊之交換， <b>建立</b> 適當之交換程序及安全保護措施，以 <b>確保</b> 資訊之完整性及機密性（如 <b>採行</b> 識別碼通行碼管制、電子資料加密或電子簽章認證等）？是否 <b>針對</b> 重要資料的交換過程， <b>保存</b> 適當之監控紀錄？				
7.15	是否 <b>建立</b> 帳號管理機制，並 <b>定期</b> 盤點？使用預設密碼 <b>登入</b> 資通系統時，是否於登入後 <b>要求</b> 立即變更密碼，並 <b>規定</b> 密碼強度、更換週期（限制使用弱密碼）？是否是最小權限？是否有使用角色型存取控制？有管理者權限之帳號是否有只用於管理活動？				
7.16	是否 <b>針對</b> 電腦機房及重要區域之安全控制、人員進出管控、環境維護（如溫溼度控制）等項目 <b>建立</b> 適當之管理措施，且 <b>落實</b> 執行？				
7.17	是否 <b>定期</b> 評估及檢查重要資通設備之設置地點可能之危害因素（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）？				

7.18	是否針對電腦機房及重要區域之公用服務（如水、電、消防及通訊等）建立適當之備援方案？
7.19	是否訂定資訊處理設備作業程序、變更管理程序及管理責任（如相關儲存媒體、設備是否有安全處理程序及分級標示、報廢程序等），且落實執行？是否訂定資訊設備回收再使用及汰除之安全控制作業程序，以確保任何機密性或敏感性資料已確實刪除？
7.20	是否針對使用者電腦訂定軟體安裝管控規則？是否確認授權軟體及免費軟體之使用情形，且定期檢查？
7.21	是否針對個人行動裝置及可攜式媒體訂定管理程序，且落實執行，並定期審查、監控及稽核？
7.22	是否有網路即時通訊管理措施（如機密公務或因處理公務上而涉及之個人隱私資訊，不得使用即時通訊軟體處理及傳送等）？是否有即時通訊軟體安全需求及購置準則？
7.23	<p>【適用行政院所屬公務機關，不論資安責任等級】機關所維運對外或為民服務網站，是否採取相關 DDoS 防護措施（例如靜態網頁切換、CDN、流量清洗或建置 DDoS 防護設備等），並確認其有效性？</p> <p>【適用特定非公務機關】</p>
7.24	機關是否對雲端服務應用進行相關資安防護管理？