

附表四

國軍資通系統防護基準確認書

資通系統防護需求等級：普 中 高

填表日期： 年 月 日

本系統是否含有個人資料：是 否

系統名稱					
計畫申購單位		承辦人		單位主管	

※本表單依「資通安全責任等級分級辦法」第十一條第二項「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」之要求，確認附表十所訂各項措施符合情形。

※本確認書以符合資安法要求為原則，爾後有需要再滾動修正。

※計畫申購單位應依系統安全等級將相應之資通安全管控措施項目提出說明：

1. 等級為「普」之系統，須填寫等級「普」之項目。
2. 等級為「中」之系統，須填寫等級「普、中」之項目。
3. 等級為「高」之系統，須填寫全部項目。

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
1.存取控制	1-1.帳號管理	1	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。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統帳號申請、開通、停用及刪除機制採用（複選）： <input type="checkbox"/> 填寫紙本申請單流程（如：帳號權限申請表（SSO）、XXX 應用系統使用者帳號異動申請單） <input type="checkbox"/> 系統線上申請流程 <input type="checkbox"/> 其他，程序說明_____
		2	已逾期之臨時或緊急帳號應刪除或禁用。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 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，皆採最小權限原則。 2. 系統最近一次帳號清查：____年__月__日
		3	資通系統閒置帳號應禁用。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	
		4	定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
1.存取控制	1-1.帳號管理	5	逾越機關所定預定期間置時間或可使用期限時，系統應自動將使用者登出。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統閒置時間設為_____分鐘後系統會自動登出。 2. 是否有限制使用者登入時段(如:上班時): <input type="checkbox"/> 有 限制時段:_____ <input type="checkbox"/> 無
		6	應依機關規定之情況及條件，使用資通系統。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統配合本部所定之情況及條件(如指定IP來源)，限制使用說明: _____
		7	監控資通系統帳號，如發現帳號違常使用時回報管理者。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統回報方式: _____
	1-2.最小權限	8	採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 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，皆採最小權限原則。 2. 系統最近一次帳號清查:____年__月__日
	1-3.遠端存取	9	自單位內採連線存取，應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。 ※依本部資安政策，不允許遠端(自單位外連入)存取	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	<input type="checkbox"/> 本系統未開放遠端存取及單位內連線存取功能 <input type="checkbox"/> 本系統廠商可於單位內以連線存取方式連至後台管理頁面，管控機制: _____(如:限定連接電腦IP)

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
2.稽核與可歸責性	2-1.稽核事件	10	依規定時間週期及紀錄留存政策，保留稽核紀錄。(應用系統稽核紀錄保存至少1年、含個人資料者保存至少5年)	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統目前保留最早之應用系統稽核紀錄為____年____月____日之稽核紀錄；本系統保留最近一筆應用系統稽核紀錄為____年____月____日之稽核紀錄
		11	確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統至少包含更改密碼、登入成功及失敗、資訊系統存取成功及失敗等功能之稽核紀錄
		12	應稽核資通系統管理者帳號所執行之各項功能。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統提供資訊系統管理者帳號所執行之各項功能稽核日誌
		13	應定期審查稽核事件。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統最近一次審核稽核事件日期：____年____月____日
	2-2.稽核紀錄內容	14	資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	稽核日誌已具備以下項目： (1)識別使用者之ID，不可為個資類型。 (2)時間應記錄至秒等級。 (3)執行之功能或存取資源名稱。 (4)執行結果或事件描述。 (5)網路來源與目的位址。
		15	資通系統產生之稽核紀錄，應依需求納入其他相關資訊。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	除事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊外，本系統是否有納入其他相關資訊之需求： <input type="checkbox"/> 無 <input type="checkbox"/> 有，已納入其他相關資訊
	2-3.稽核儲存容量	16	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已配置稽核紀錄所需之儲存容量，儲存容量超過警示值將以e-mail通報應用系統承辦人員。

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
2.稽核與可歸責性	2-4.稽核處理失效之回應	17	資通系統於稽核處理失效時，應採取適當之行動。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統稽核處理失效(註1)時處理方式為： <input type="checkbox"/> 關閉資訊系統 <input type="checkbox"/> 覆寫最舊的稽核紀錄 <input type="checkbox"/> 停止產生稽核紀錄 <input type="checkbox"/> 通知管理者進行故障排除 <input type="checkbox"/> 其他 _____
		18	機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統稽核失效(註1)時的通報機制採用： <input type="checkbox"/> email <input type="checkbox"/> 簡訊 <input type="checkbox"/> 其他 _____ 2. 通報人員：_____
	2-5.時戳及校時	19	資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統稽核紀錄時戳，_____ (系統內部時鐘或本部 NTP 伺服器)產生，可對應至 _____ (UTC 或 GMT)
		20	系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統主機時間與應用系統管理人員個人電腦時間相符
	2-6.稽核資訊之保護	21	對稽核紀錄之存取管理，僅限於有權限之使用者。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	稽核日誌僅特定授權之人員： _____ (如：系統管理人員)才得以存取。
		22	應運用雜湊或其他適當方式之完整性確保機制。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	稽核紀錄運用雜湊或其他適當方式確保其完整性，管控機制：_____ (如：異機備份稽核紀錄、稽核紀錄匯出時提供 Hash 值)

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
2.稽核與可歸責性	2-6.稽核資訊之保護	23	定期備份稽核紀錄至與原稽核系統不同之實體系統。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統定期備份稽核紀錄到與原系統不同之實體系統
3.營運持續計畫	3-1.系統備份	24	訂定系統可容忍資料損失之時間要求。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統可容忍資料損失時間(RPO)_____小時
		25	執行系統源碼備份。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	<input type="checkbox"/> 定期備份最新版本之系統源碼 <input type="checkbox"/> 其他_____ (套裝軟體/租賃系統可不備份系統源碼)
		26	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統最近一次備份還原測試日期：____年__月__日
		27	應將備份還原，作為營運持續計畫測試之一部分。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統最近一次營運持續演練：____年__月__日，並已包含備份還原程序
		28	應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已將資通系統軟體與其他安全相關資訊之備份置於不同處之獨立設施
	3-2.系統備援	29	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統可容忍中斷時間(RTO)_____小時
		30	原服務中斷時，於可容忍時間內，由備援設備取代提供服務。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已建置備援機制(包含 VM 備份與資料備份)，可於可容忍時間內，由備援設備取代提供服務

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
4. 識別與鑑別	4-1. 內部使用者之識別與鑑別	31	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統具備唯一識別及鑑別使用者，無共用帳號之行為
		32	對帳號之網路或本機存取採取多重認證技術。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統使用之多重認證技術： _____ (如：鎖定 IP 或使用自然人憑證)
	4-2. 身分驗證管理	33	使用預設密碼登入系統時，應於登入後要求立即變更。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統帳號預設密碼機制：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 系統無使用預設密碼，系統開通帳號程序：_____ <input type="checkbox"/> 本系統使用者以預設密碼登入系統時，於登入後要求立即變更密碼
		34	身分驗證相關資訊不以明文傳輸。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統傳遞身分驗證相關資訊(如：帳號、密碼等)採用加密傳輸，加密傳輸方式： _____ (如：採用 https 傳輸)，不以明文傳輸
		35	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少三十分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統帳戶鎖定機制：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 本系統執行帳號登入進行身分驗證失敗超過 5 次後即暫停_____分鐘(至少三十分鐘)使用者登入 <input type="checkbox"/> 其他自建登入失敗驗證機制： _____

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
4.識別與鑑別	4-2.身分驗證管理	36	基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限限制。 五、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	《內部系統》(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 非採用 SSO 登入機制： 1. 本系統通行碼長度至少 8 位字元(特權帳號 12 位字元)且包含大寫英文字母、小寫英文字母、阿拉伯數字及特殊符號等至少 3 種組合 2. 強制____個月應變更密碼(不得大於 3 個月) 3. 本系統使用者更換密碼時，不與前三次使用過之密碼相同
		37	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統防範自動化程式之登入或密碼更換嘗試機制：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 本系統防範自動化程式之登入方式：_____(如：圖形驗證)
		38	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統具有密碼重設機置：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 系統確認身分後，發送一次性及具有時效性符記 <input type="checkbox"/> 以人工確認身分，人工重設機制 <input type="checkbox"/> 其他_____
	4-3.鑑別資訊回饋	39	資通系統應遮蔽鑑別過程中之資訊。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統遮蔽在輸入過程中之資訊(如密碼於輸入時顯示為*****)

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
4.識別與鑑別	4-4.加密模組鑑別	40	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統密碼加密機制：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 非採用 SSO 登入機制： 本系統存於資料庫內之使用者密碼以加密方式(不可逆)處理儲存，以防止使用者密碼為使用者以外人員知悉。
	4-5.非內部使用者之識別與鑑別	41	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統識別及鑑別非機關使用者方式：(可複選) <input type="checkbox"/> 本系統未提供外部人員使用 <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 本系統具備識別及鑑別非機關使用者之機制，管控機制：_____ (如：帳號資訊包含使用者機關/單位) <input type="checkbox"/> 其他_____
5.系統與服務獲得	5-1.系統發展生命週期需求階段	42	針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已填寫「資通系統防護需求分級表」完成資通系統分級作業
	5-2.系統發展生命週期設計階段	43	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已填寫「防護需求等級評估表」完成資通系統分級作業
	5-3.系統發展生命週期開發階段	44	將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已依本系統「防護需求等級評估表」結果於委外需求中納入各項安全需求
	5-3.系統發展生命週期開發階段	45	應針對安全需求實作必要控制措施。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已依本系統安全等級需求進行資安法要求之控制措施

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
5.系統與服務獲得	5-3.系統發展生命週期開發階段	46	應注意避免軟體常見漏洞及實作必要控制措施。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已於開發階段避免軟體常見漏洞及實作必要控制措施，並於變更時進行驗證： <input type="checkbox"/> 本系統本年度最近一次程式變更並執行弱點掃描(檢測軟體能檢測 OWASP TOP 10)確認已無中高風險之時間:___年___月___日 <input type="checkbox"/> 本年度無進行程式變更作業，惟已於___年___月___日由資訊處協助執行弱點掃描並確認已無中高風險
		47	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	系統發生錯誤時，使用者頁面僅顯示簡短訊息及代碼不包含詳細的錯誤訊息
		48	應執行原始碼安全檢測，確認程式無安全漏洞或邏輯錯誤等風險。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已於___年___月___日完成原始碼安全檢測，檢測結果： <input type="checkbox"/> 檢測結果通過 <input type="checkbox"/> 檢測結果未通過，惟已完成程式碼修正，並於___年___月___日複測通過
	5-3.系統發展生命週期開發階段	49	執行「源碼掃描」安全檢測。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已於開發階段執行源碼掃描的時間:___年___月___日
		50	具備系統嚴重錯誤之通知機制。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統嚴重錯誤(如：使系統營運中斷)之通知機制： <input type="checkbox"/> email <input type="checkbox"/> 簡訊 <input type="checkbox"/> 其他_____
	5-4.系統發展生命週期測試階段	51	執行「弱點掃描」安全檢測。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已執行「弱點掃描」，並確認已無中高風險或已接受無法修補風險之時間:___年___月___日(掃描時間須驗收前1個月內)
		52	執行「滲透測試」安全檢測。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統最近一次依滲透測試結果修補並確認已無中高風險或已接受無法修補風險之時間:___年___月___日(至少每年須辦理1次)
	5-5.系統發展生命週期部署與維護階段	53	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. <input type="checkbox"/> 本系統主機為 Windows 系統，由資訊處協助更新及修補(Patch) <input type="checkbox"/> 本系統主機為 Linux 系統/其他作業系統，最近一次針對資通安全威脅或弱點執行更新或修補(Patch)的時間:___年___月___日 2. 已開啟本機防火牆，並關閉不必要服務及

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
						埠口，目前開啟 Port：_____
5.系統與服務獲得	5-5.系統發展生命週期部署與維運階段	54	資通系統相關軟體，不使用預設密碼。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統相關軟體未使用預設密碼
		55	於系統發展生命週期之維運階段，須注意版本控制與變更管理。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統使用的版本控管機制為：_____ 2. 本系統依「系統獲取開發與維護管理規範」填寫「正式作業變更管制紀錄表」進行變更管理
	5-6.系統發展生命週期委外階段	56	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已填寫「防護需求等級評估表」完成資通系統分級作業，並將安全需求納入本系統需求書
	5-7.獲得程序	57	開發、測試及正式作業環境應為區隔。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統開發、測試及正式作業環境皆有區隔
	5-8.系統文件	58	應儲存與管理系統發展生命週期之相關文件。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統皆有儲存與管理系統發展生命週期之相關文件_____（如：系統設計分析文件、系統維護文件、操作手冊）
6.系統與通訊保護	6-1.傳輸之機密性與完整性	59	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已採用 Https 加密機制，並使用合法憑證中心(政府憑證管理中心 GCA 或國軍憑證管理中心 MCA)核發之伺服器憑證。
		60	使用公開、國際機構驗證且未遭破解之演算法。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已採用 Https 加密機制，並使用合法憑證中心(政府憑證管理中心 GCA 或國軍憑證管理中心 MCA)核發之伺服器憑證。
		61	支援演算法最大長度金鑰。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已採用 Https 加密機制，並使用合法憑證中心(政府憑證管理中心 GCA 或國軍憑證管理中心 MCA)核發之伺服器憑證。

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
6.系統與通訊保護	6-1.傳輸之機密性與完整性	62	加密金鑰或憑證週期性更換。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	憑證及金鑰的有效期限:____年__月__日
		63	伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已依本部「密碼措施管理規範」實施應有之安全防護措施
	6-2.資料儲存之安全	64	靜置資訊及相關具保護需求之機密資訊應加密儲存。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統靜置資訊(如應用系統設定之備份檔)及相關具保護需求之機密資訊已加密儲存
7.系統與資訊完整性	7-1.漏洞修復	65	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統依最近一次資訊業管單位弱點掃描結果修補並確認已無中高風險或已接受無法修補風險之時間:____年__月__日
		66	定期確認資通系統相關漏洞修復之狀態。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	
	7-2.資通系統監控	67	發現資通系統有被入侵跡象時，應通報機關特定人員。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	如發現資通系統有被入侵跡象，將通知資訊部門。
		68	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1.本系統已納入SOC監控偵測攻擊(由資訊業管單位統一辦理) 2.本系統已保留嘗試錯誤(登入失敗)之稽核紀錄識別系統之未授權使用
		69	資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統自動化工具監控機制： _____

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
7.系統與資訊完整性	7-3.軟體及資訊完整性	70	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統重要程式已採完整性驗證機制：_____（如：SVN），偵測未授權變更特定軟體及資訊
		71	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統使用者輸入資料合法性檢查應置放於應用系統伺服器端（對於使用者輸入欄位資料，僅允許特定之內容，並於伺服器端檢查）
	7-3.軟體及資訊完整性	72	發現違反完整性時，資通系統應實施機關指定之安全保護措施。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	如發現違反完整性時（如：資料或程式遭竄改），資通系統將進行回復作業
		73	應定期執行軟體與資訊完整性檢查。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統檢查週期為：_____（每年/季/月） 2. 最近一次執行特定軟體與資訊完整性檢查：____年__月__日

註：稽核處理失效包括：軟/硬體錯誤、稽核擷取機制失效、稽核儲存容量飽和或超過。可採取下列額外的行動，例如：關閉資訊系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等。