資通系統資安防護基準要求與查核表

專案名稱：_____ 日期： 年 月 日

廠商名稱：_____

填寫人：_____ 審查人：_____

系統名稱：_____ 安全等級：□普 □中 □高

請依據貴管資通系統之安全等級，填寫勾選項目之執行情形或佐證資料，未勾選項目毋須填列。

存取控制

帳號管理(Account Management)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明 1、灰色字體為填表說明，請各系統依實際執行情形填寫。 2、黑色字體表共通作業部分，毋須個別填寫。 3、左欄勾選不適用者，請說明原因。
	普	中	高		
建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統帳號管理程序，並說明是否保留帳號新增、停用、或刪除等申請表單紀錄。
已逾期之臨時或緊急帳號應刪除或禁用。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統對於臨時或緊急帳號之管理程序。
資通系統閒置帳號應禁用。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明閒置帳號禁用方式，是否定期辦理帳號清查並留下清查紀錄。
定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否定期辦理帳號清查並留下清查紀錄。
機關應定義各系統之閒置時間或可使用期限及資通系統之使用情況及條件。			V	☑是 □不適用 □否，預計完成時間 年 月 日	已定義於「ISMS-4-042 應用系統安全需求查檢表」，使用者帳號至多 30 分鐘內未活動即自動失效。
逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。			V	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否依規定設置系統閒置超時自動登出機制、設置時間為多久？
應依機關規定之情況及條件(如上班時間或指定 IP 來源)使用資通系統。			V	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否有系統使用時間規定、遠端連線來源 IP 限制？
監控資通系統帳號，如發現帳號違常使用時回報管理者。			V	□是 □不適用 □否，預計完成時間 年 月 日	1.本署系統安全等級「高」之系統已透過 SOC 監控系統帳號登入情形，如有異常立即通知相關人員。 2.請說明系統本身是否有未經授權登入系統之監控及通報機制？機制為何？

最小權限(Least Privilege)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
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。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否依據權責設置帳號權限？

遠端存取(Remote Access)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	1.維護廠商遠端存取需先填寫「ISMS-4-017 資訊作業申請單」，經核准後以限制 IP 方式提供使用。 2.請說明使用者透過 HTTPS、SSH、VPN 等存取系統之授權及遠端存取管理機制？ (系統主機非存置本署，請就 1、2 項說明)
使用者之權限檢查作業應於伺服器端完成。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明使用者之權限檢查是否於伺服器端完成？
應監控遠端存取機關內部網段或資通系統後台之連線。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	本署透過 SOC、WAF 監控，並以 Observed IT 側錄軟體監控廠商遠端連線之操作行為，並發遠端連線訊息郵件通知系統承辦人。 (系統主機非存置本署，請說明監控方式)
應採用加密機制。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統或 RDP 遠端連線是否採加密安全通道，如 TLS1.2、RPC 通訊等。
遠端存取之來源應為機關已預先定義及管理之存取控制點。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	1.本署系統遠端維護採限定來源 IP 位址、限定連線 PORT、限定連線時間之方式提供使用。 2.請說明系統本身遠端存取機制、如設定 Windows IIS 白名單、防火牆限臺灣 IP 等。 (系統主機非存置本署，請就 1、2 項說明)

事件日誌與可歸責性

記錄事件(Audit Events)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	V	V	V	□是 □不適用 □否，預計完成時	請說明日誌(Log)保存方式與保存時間(依本署規定，

				間　年　月　日	紀錄之保存期限須考量組織需求與法令法規要求，若無特別規定，至少須保存6個月)。
確保資通系統有記錄特定事件(如更改密碼、登錄失敗、資通系統存取失敗)之功能，並決定應記錄之特定資通系統事件。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明系統是否收集如左列特定事件之紀錄(log)，且於特定事件發生或發生次數異常時，是否發出異常警訊以供系統管理員查核？
應記錄資通系統管理者帳號所執行之各項功能。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明對管理者帳號所為之各種操作是否留下稽核紀錄？
應定期審查機關所保留資通系統產生之日誌。		V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明是否留下定期審查日誌紀錄(log)之佐證資料？

日誌紀錄內容(Content of Audit Records)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統產生之日誌應包含事件類型、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，並採用單一日誌紀錄機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明日誌紀錄是否包含左列安全需求，並採用單一(格式一致)的 Log 機制並依要求納入額外稽核紀錄？

日誌儲存容量(Audit Storage Capacity)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
依據日誌紀錄儲存需求，配置所需之儲存容量。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明是否已配置所需之日誌儲存容量？

日誌處理失效之回應(Response to Audit Processing Failures)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統於日誌處理失效時，應採取適當之行動。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明當系統記錄稽核紀錄之作業失效時，處理方式為何？
機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。			V	□是 □不適用 □否，預計完成時間　年　月　日	請說明特定稽核失效事件(資安事件達 1 級(含)以上)發生時，系統是否在 1 小時內通知相關權責人員？

時戳及校時(Time Stamps)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應使用系統內部時鐘產生日誌紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	本署各系統主機定時與本署校時主機進行校時，基準時間源為國家時間與頻率標準實驗室。 (系統主機非存置本署，請說明校時機制為何？)
系統內部時鐘應定期與基準時間源進行同步。		V	V	□是 □不適用 □否，預計完成時間　年　月　日	

日誌資訊之保護(Protection of Audit Information)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
對日誌紀錄之存取管理，僅限於有權限之使用者。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明日誌紀錄的存取限制方式為何？(如僅提供特定權限人員可透過系統介面查詢)
應運用雜湊或其他適當方式之完整性確保機制。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統是否提供雜湊或其他方式確保日誌完整性，避免日誌遭竄改？
定期備份日誌至原系統外之其他實體系統。			V	□是 □不適用 □否，預計完成時間 年 月 日	儲存於資料庫之稽核紀錄，有採異地備份機制，餘網站服務 log、system log 等，則另備份於與系統不同實體之儲存媒體上。 (系統主機非存置本署，請說明備份機制為何？)

營運持續計畫

系統備份(Information System Backup)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
訂定系統可容忍資料損失之時間要求。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	系統主機存置於本署可容忍資料損失時間(RPO)為24 小時。 (系統主機非存置本署，請說明可容許損失資料之時間(RPO)為何？)
執行系統源碼與資料備份。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	源碼備份：每季(期)由廠商交付光碟備份。 系統備份：每日備份，保留 7 日。 資料庫備份：每日完整備份，每小時交易紀錄檔備份，保留 1 個月。 (系統主機非存置本署，請說明備份機制。)
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。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	系統主機存置於本署，依本署營運持續演練規劃辦理。 (系統主機非存置本署，請說明是否定期執行備份還原演練？)
應將備份還原，作為營運持續計畫測試之一部分。			V	☑是 □不適用 □否，預計完成時間 年 月 日	本署之營運持續演練，有將系統及資料庫備份還原納為執行項目，詳如營運持續演練計畫及報告。
應在與運作系統不同地點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。			V	□是 □不適用 □否，預計完成時間 年 月 日	重要資通系統軟體與其他安全相關資訊之備份另外儲存於非伺服器本身的位置，且資料庫備份檔有異地備份措施。

					(系統主機非存置本署，請說明系統及資料是否異地存放？)

系統備援(Redundancy of Information Systems)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
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。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	可容許資通系統中斷時間為(RTO)： ___小時。(請依系統安全等級評估表之可用性填寫對應數值。(填寫值：8 小時(高)、24 小時(中)、72 小時(普)) 註：應與資通系統安全等級評估表、營運衝擊分析表、及合約中之服務水準協議(SLA)一致
原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	可由備份還原或全機重建方式於可容忍中斷時間內提供服務。 (系統主機非存置本署，請說明還原機制可否於可容忍時間內提供服務。)

識別與鑑別

內部使用者之識別與鑑別(Identification and Authentication)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
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。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統機制是否可唯一識別且足供鑑別機關內部使用者，禁止使用共用帳號？
對資通系統之存取採取多重認證技術。			V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統是否具備多重認證或鎖定 IP 機制？

身分驗證管理

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
使用預設密碼登入系統時，應於登入後要求立即變更。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	新帳號登入時是否要求變更預設密碼？
身分驗證相關資訊不以明文傳輸。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	帳密驗證資料傳輸時是否有加密？
具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五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。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	帳密驗證失敗的鎖定方式為何？
使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(非內部使用者，可依機關自行規範辦理。)	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	密碼複雜度與效期是否有要求？

密碼變更時，至少不可以與前三次使用過之密碼相同。(非內部使用者，可依機關自行規範辦理。)	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	更換密碼是否有歷程之要求？
身分驗證機制應防範自動化程式之登入或密碼更換嘗試。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	身分驗證是否有防止自動化方式登入(例如增加圖形驗證碼之輸入)？
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。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	密碼重設時發送之驗證過程(如:驗證碼、驗證連結)是否有時效限制？

鑑別資訊回饋(Authenticator Feedback)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應遮蔽在鑑別過程中之資訊(如通行碼)，以防止未授權之使用者可能之窺探/使用。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	系統登入時之密碼或機敏鑑別資訊是否不以明文顯示？

加密模組鑑別(Cryptographic Module Authentication)

安全需求檢核項目	資訊系統資安等級			符合度	佐證資料或作法說明
	普	中	高		
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。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	密碼是否加密或經雜湊處理後儲存？

非內部使用者之識別與鑑別(Identification and Authentication)

安全需求檢核項目	資訊系統資安等級			符合度	佐證資料或作法說明
	普	中	高		
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)。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統機制是否可識別且足供鑑別機關內、外部使用者？

系統與服務獲得

系統發展生命週期需求階段(System Development Life Cycle-Requirement)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
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。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	依據資通安全責任等級分級辦法附表九規定先評定系統資安等級，再使用「應用系統安全需求查檢表」進行安全需求確認。

系統發展生命週期設計階段(System Development Life Cycle-Design)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
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。		V	V	☑是 □不適用 □否，預計完成時間 年 月 日	各系統先進行高階風險評鑑(依據資通安全責任等級分級辦法附表九規定，評定系統資安等級)，資訊系統安全等級鑑別為高者或資訊資產安全等級為高者，再進行細部風險評鑑作業(風險評估表)。
將風險評估結果回饋需求階段之檢核項目，並		V	V	□是 □不適用	是否將風險評估結果回饋

提出安全需求修正。				□否，預計完成時間　年　月　日	至應用系統安全需求查檢表？

系統發展生命週期開發階段(System Development Life Cycle-Develop)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
應針對安全需求實作必要控制措施。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	是否已依系統安全等級實作必要控制措施？
應注意避免軟體常見漏洞及實作必要控制措施。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	是否定期執行資安檢測、code review 確保無常見漏洞？如定期交付資安檢測報告及漏洞修補。
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。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明系統是否已避免於系統錯誤時顯示詳細錯誤訊息(如明確指出是帳號或密碼錯誤)，以免有心人士得知系統太多細節？
執行「源碼掃描」安全檢測。			V	□是 □不適用 □否，預計完成時間　年　月　日	系統上線前是否有源碼檢測紀錄？
系統應具備發生嚴重錯誤時之通知機制。			V	□是 □不適用 □否，預計完成時間　年　月　日	系統在嚴重錯誤時是否有通知機制？機制為何？

系統發展生命週期測試階段(System Development Life Cycle-Test)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
執行「弱點掃描」安全檢測。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	是否有弱點掃描紀錄？
執行「滲透測試」安全檢測。			V	□是 □不適用 □否，預計完成時間　年　月　日	是否有滲透測試紀錄？

系統發展生命週期部署與維運階段(System Development Life Cycle-Deployment and Maintenance)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
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。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	主機作業系統由機房統一處理更新及修補事宜，相關服務或埠口視系統需要提出申請並經核准始能開啟。 (系統主機非存置本署，請說明服務或埠口管理方式？)
資通系統相關軟體， 不使用預設密碼。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	1.機房使用之相關管理工具皆已變更密碼。 2.請說明資通系統使用之相關軟體是否使用預設密碼？ (系統主機非存置本署，請就 1、2 項說明)
於系統發展生命週期之維運階段，應執行版本		V	V	□是 □不適用	版本版次之管理方式為

控制與變更管理。				□否，預計完成時間　年　月　日	何？系統變更是否填寫變更申請單？

系統發展生命週期委外階段(System Development Life Cycle-Outsourcing)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
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。	V	V	V	☑是 □不適用 □否，預計完成時間　年　月　日	資訊作業委外採用工程會之資訊服務採購契約，且將應用系統安全需求指引及需求查檢表納入委外合約中，請廠商依據系統資安等級實作各項安全控制措施。

獲得程序(Acquisition Process)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
開發、測試及正式作業環境應為區隔。		V	V	□是 □不適用 □否，預計完成時間　年　月　日	開發、測試及正式環境是否區隔？

系統文件(Information System Documentation)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
應儲存與管理系統發展生命週期之相關文件。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	資訊系統從評估、規劃、招標、建置乃至維運過程之相關文件是否妥善保存？

系統與通訊保護

傳輸之機密性與完整性(Transmission Confidentiality and Integrity)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
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。			V	□是 □不適用 □否，預計完成時間　年　月　日	網站傳輸資料時，是否採用HTTPS(透過 SSL 或 TLS 等加密協定)協定以確保資料以密文方式傳輸？
使用公開、國際機構驗證且未遭破解之演算法。			V	□是 □不適用 □否，預計完成時間　年　月　日	不使用自行創造的加密方式，採用公開、國際認可之演算法，例如 AES、RSA 及 SHA 安全雜湊等演算法。
支援演算法最大長度金鑰。			V	□是 □不適用 □否，預計完成時間　年　月　日	請說明系統採用之密碼學演算法，是否使用該演算法目前支援的最大金鑰長度，以減少被暴力破解之可能。例如 AES 256 bits、RSA 2048 bits 、SHA-512 等或以上。
加密金鑰或憑證應定期更換。			V	☑是 □不適用 □否，預計完成時間　年　月　日	依據 GCA 政府憑證管理中心所核發憑證之有效期限，定期辦理憑證更新。
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。			V	□是 □不適用 □否，預計完成時	請說明針對使用的金鑰是否以密碼保護，並進行備

				間　年　月　日	份及妥善保管；且加密金鑰不與加密資料存放於同一系統中，並對於加密金鑰的存取進行限制。

資料儲存之安全(Protection of Information at Rest)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。			V	□是 □不適用 □否，預計完成時間　年　月　日	請說明系統是否已定義哪些資料屬機密資料？其於資料庫或其他儲存裝置上是否加密儲存？以減少機敏資料因儲存媒體或裝置有其他存取管道而洩漏的風險。

系統與資訊完整性

漏洞修復(Flaw Remediation)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
系統之漏洞修復應測試有效性及潛在影響，並定期更新。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明是否針對系統漏洞進行影響評估並定期更新修補？
定期確認資通系統相關漏洞修復之狀態。		V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明是否定期確認系統漏洞修復之狀態？

資通系統監控(Information System Monitoring)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
發現資通系統有被入侵跡象時，應通報機關特定人員。	V	V	V	☑是 □不適用 □否，預計完成時間　年　月　日	依本署資訊安全事件管理規範及系統委外需求書對廠商資安通報之要求辦理。
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。		V	V	□是 □不適用 □否，預計完成時間　年　月　日	使用 SOC 及應用系統防火牆(WAF)監控資通系統，以偵測攻擊與未授權之連線，並分析每週 WAF 攻擊阻擋來源 TOP5、確認惡意攻擊 IP 並於防火牆設定，加以阻擋。 (系統主機非存置本署，請說明監控機制為何？)
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。			V	□是 □不適用 □否，預計完成時間　年　月　日	使用 SOC 及應用系統防火牆(WAF)監控資通系統，並進行事件分析。 (系統主機非存置本署，請說明是否對系統進出流量進行監控，於發現異常時之處置為何？)

軟體及資訊完整性(Software, Firmware, and Information Integrity)

安全需求檢核項目	資訊系統資安等級	是否符合	佐證資料或作法說明

	普	中	高		
使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	系統程式目錄已透過 SVN 監控偵測機制，確保程式、設定檔不被未經授權者變更。 (系統主機非存置本署，請說明是否使用完整性驗證工具偵測軟體或資訊是否遭受未經授權之變更？)
使用者輸入資料合法性檢查應置放於應用系統伺服器端。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明對於使用者輸入欄位資料，是否於伺服器端進行合法性檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法？
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。		V	V	☑是 □不適用 □否，預計完成時間 年 月 日	當軟體與資訊經發現違反完整性時，依據本署資通安全事件通報及應變管理規範進行通報，並即刻停止系統服務，經追查原因、復原系統及資料後，方能繼續系統服務。
應定期執行軟體與資訊完整性檢查。			V	□是 □不適用 □否，預計完成時間 年 月 日	是否定期執行軟體與資訊完整性檢查並留下紀錄？