SSDLC採取措施及驗證查核表

系統名稱：	捐款網站系統	機密性：	高		檢核日期：
功能說明：	線上捐款資訊及交易作業	完整性：	中		
		可用性：	中		
		法遵性：	高		
業務單位：	發展策劃部	防護需求等級：			

序號	構面	控制措施	安全需求項目	說明	本法人規範	普	中	高	類別	採取措施	驗證方式	驗證結果	備註
1	存取控制	帳號管理	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。	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、建立、修改、開通、停用或刪除之行為。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	系統管理員為發展部， 帳號以資服單申請及管制。	檢視本系統之權限申請單。		
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。	資訊服務帳號及密碼管理 B-04-33-00-B2040		中	高	技術	因無臨時帳號配發作業， 每年權限審核維運措施管控。	檢視本系之年度權審紀錄。		
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。	資訊服務帳號及密碼管理 B-04-33-00-B2040		中	高	技術	每年權限審核維運措施管控。	檢視本系之年度權審紀錄。		
4			定期審核資通系統帳號之建立、修改、啟用、停用及刪除	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，並停用或刪除閒置帳號與臨時帳號。	資訊服務帳號及密碼管理 B-04-33-00-B2040		中	高	維運	每年權限審核維運措施管控。	檢視本系之年度權審紀錄。		
5			機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件例如帳號 類型與功能限制、操作時段限制、來源位址、連線數量及存取資源等 。	定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件例如帳號 類型與功能限制、操作時段限制、來源位址、連線數量及存取資源等 。	資訊專案管理 C-04-33-00-C1020 網站維護合約			高	技術	要求合約廠商實施閒置登出功能。	實機測試閒置5分鐘，確認系統已登出。		
6			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	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。	資訊專案管理 C-04-33-00-C1020 門諾公益勸募網維護合約：2019~2024			高	技術	要求合約廠商實施閒置登出功能。	實機測試閒置5分鐘，確認系統已中斷連線。		
7			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)。	遠端連線服務管理規範 C-04-33-00-E1040			高	技術	限制管理者自院外連至主機後台作業時, 須安裝 SSL VPN 端點防護系統。	抽查院外登入紀錄。		
8			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)。	資訊專案管理 C-04-33-00-C1020 網站維護合約			高	技術	由開發廠商實作，網站管理後台登入異常之日誌及回報機制。	請系統開發者提供佐證資訊。		
9		最小權限	採用最小權限原則，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	使用者(或代表使用者行為之程序)應以完成該工作所需的最小權限操作系統功能，避免過度授權而增加系統資源被不當存取的風險。因此在進行授權決定時，應考量該使用者(或代表使用者行為之程序)之業務性質與範圍，限制其所能存取的系統功能及資料。	資訊服務帳號及密碼管理 B-04-33-00-B2040		中	高	維運	每年權限審核維運措施，由單位主管審檢視是否過度授權。	檢視本系之年度權審紀錄。		
10		遠端存取	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	機關應明確訂定資通系統之存取限制、組態需求、連線需求，並將這些資訊文件化，以供日後查檢。	遠端連線服務管理規範 C-04-33-00-E1040	普	中	高	技術	廠商連線須以Citrix +OTP 管制作業連線。	抽察廠商維護之連線紀錄。		
11			使用者之權限檢查作業應於伺服器端完成	應於伺服器端實作權限檢查機制，並預設禁止任何未通過權限檢查之存取行為，以避免被使用者繞過。	資訊專案管理 C-04-33-00-C1020 網站維護合約	普	中	高	技術	由開發廠商實作權限檢查機制。	確認捐款後台作業必須先有權限驗證才能存取網站功能。		
12			應監控遠端存取機關內部網段或資通系統後臺之連線	資通系統所允許之遠端連線活動，應使用監控設備或其他可偵測未經授權使用的設備，在發現異常連線或存取行為時提出警告，以防止資通系統被不當使用。	網路管理規範 B-04-33-00-B1012	普	中	高	維運	門諾公益捐款網站納入WAF內部，以偵測異常連線或存取行為。	由WAF管理者提供佐證資訊。		
13			應採用加密機制	遠端存取資通系統時，應以加密機制保護機敏資料傳輸時之機密性。常見作法如採用HTTPS加密傳輸等，並選擇高強度之協定版本及演算法。	資訊服務管理 B-04-33-00-A2030	普	中	高	技術	門諾公益捐款網站, 僅能以 https 運作。	驗證捐款網站憑證效期。		

序號	構面	控制措施	安全需求項目	說明	本法人規範	普	中	高	類別	採取措施	驗證方式	驗證結果	備註
14			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	遠端存取行為應經過適當授權後始可放行，若有必要允許外部遠端存取之系統功能，應限制資通系統遠端存取之來源(如機器、網路位址等)，預先定義合法來源並進行管理，避免全面性開放存取。	網路管理規範 B-04-33-00-B1012		中	高	維運	門諾公益捐款網站納入WAF內部，並限制特定IP(發展部) 才能連上後台網站。	確認僅有特定的IP 才能連上後台網站。		
15	事件日誌與可歸責性	記錄事件	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	應依規定之時間週期及紀錄留存政策，保留系統日誌紀錄(Audit Logs)，目的包含程式除錯、行為歸責、稽核取證及法規要求等。	紀錄管制程序 B-04-33-00-B1023	普	中	高	技術	固定以 Kiwi Server 接收日誌	由Kiwi 管理員提供捐款網站日誌記錄佐證資訊。		
16			確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件	資通系統應有記錄特定事件之功能，如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等。	紀錄管制程序 B-04-33-00-B1023	普	中	高	技術	固定以 Kiwi Server 接收日誌	由Kiwi 管理員提供捐款網站日誌記錄佐證資訊。		
17			應記錄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，記錄所有管理者帳號執行之各項功能，有助於定期稽核系統行為及資安事件追查。	紀錄管制程序 B-04-33-00-B1023	普	中	高	技術	固定以 Kiwi Server 接收日誌	由Kiwi 管理員提供捐款網站日誌記錄佐證資訊。		
18			應定期審查機關所保留資通系統產生之日誌	機關應訂定日誌審查時程**(每季)**，由負責人員檢視日誌紀錄內容，以掌握是否在期間內曾發生重要的資安事件，如異常的存取行為、重大的系統錯誤等。	紀錄管制程序 B-04-33-00-B1023		中	高	維運	應有定期審核重要日誌。	應有定期審核重要日誌。		
19		日誌紀錄內容	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。	日誌紀錄應包含下列項目，並得視系統業務狀況調整： （1）使用者ID(不可為個資類型)。 （2）經系統校時後之時間戳記。 （3）執行之功能或存取之資源名稱。 （4）事件類型或優先等級(priority)。 （5）執行結果或事件描述。 （6）事件發生當下相關物件資訊。 （7）網路來源及目的位址。 （8）錯誤代碼。 採用單一的日誌紀錄機制，如同一伺服器軟體應產出相同格式之日誌紀錄等，以便於事件比對與追查。 日誌紀錄應依據法律政策或業務使用等需求，納入其他相關資訊，如憑證資訊、會談識別碼等。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	技術	由開發廠商實作應用系統，依重要作業產出日誌紀錄。	驗證捐款網站系統產生之日誌記錄。		
20		日誌儲存容量	依據日誌紀錄儲存需求，配置所需之儲存容量	資通系統應配置日誌紀錄所需之儲存容量(如磁碟或資料庫空間等)，避免因儲存容量不足造成日誌處理失效。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	管理	以ServerAlive 監控應用系統服務主機儲存容量	驗證捐款網站儲存空間低於或值時會發出警訊。		
21		日誌處理失效之回應	資通系統於日誌處理失效時，應採取適當之行動	日誌處理失效時，應訂定相對應的處理措施，如覆寫最舊的日誌紀錄、停止產生日誌紀錄或對特定人員提出警告等，避免危害系統可用性，或是當資安事件發生時無日誌紀錄可比對追查之情況。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	技術	由開發廠商實作應用系統，提出當日誌紀錄失效之警示機制。	驗證捐款網站系統產生日誌記錄作業，失效時之警示機制。		
22			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	應定義需要即時通報的特定日誌失效事件、即時通報的時效以及特定通知對象，並實作通知機制，以利及早釐清事件發生原因並進行故障排除。如當日誌紀錄無法正常寫入資料庫時，以信件或簡訊通知系統維護人員。	N.A.			高	技術				
23		時戳及校時	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)	使用系統內部時鐘(本法人之鐘訊主機)產生稽核紀錄所需時戳，採用全系統一致的時間標準，有助於彙整資安事件所發生的各種事件時間點，進而分析資安事件可能發生的原因。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	技術	由開發廠商實作應用系統，採用一致的時間標準。	驗證捐款網站系統產出時間與標準時間一致。		
24			系統內部時鐘應定期與基準時間源進行同步	日誌紀錄必須維持使用精確的時間，以利事件追蹤及稽核取證等用途，實務上，可使用網路時間協定(Network Time Protocol, NTP)，讓機關內各個系統及網路設備與校時伺服器進行同步，如國家標準時間伺服器(time.stdtime.gov.tw)或使用機關自建之伺服器。	資訊機房設置及管理 B-04-33-00-E1001			中	高	技術	捐款網站主機納入AD 管制，統一與DC 對時。	驗證捐款網站主機時間與標準時間一致。		

序號	構面	控制措施	安全需求項目	說明	本法人規範	普	中	高	類別	採取措施	驗證方式	驗證結果	備註
25		日誌資訊之保護	對日誌紀錄之存取管理，僅限於有權限之使用者	應施行日誌紀錄存取控管，避免未經授權使用者惡意讀取、竄改或刪除稽核紀錄。	紀錄管制程序 B-04-33-00-B1023	普	中	高	技術	固定以 Kiwi Server 接收日誌	由Kiwi 管理員提供捐款網站日誌記錄佐證資訊。		
26			應運用雜湊或其他適當方式之完整性確保機制	日誌資訊以安全雜湊演算法產生，並留存其雜湊值，後續可對資料再次產生雜湊值並與原先結果進行比對，以確保資料未遭到異動竄改。	紀錄管制程序 B-04-33-00-B1023		中	高	技術	導入日誌完整性保全作業。	導入日誌完整性保全作業。		
27			定期備份日誌至與原系統外之其他實體系統	定期將日誌紀錄備份至與原系統不同之實體系統，如建置Log伺服器或設定系統排程等方式，集中管理及保存日誌紀錄之備份，可降低因系統損毀或人為惡意刪除而無法取用日誌紀錄之風險。	N.A.			高	技術				
28	營運持續計畫	系統備份	訂定系統可容忍資料損失之時間要求	機關應訂定可容忍資料損失之時間要求，若資安事件發生造成資料損失時，需使用最接近的備份資料進行復原，資料損失與備份資料之間的時間間隔，亦稱為復原點目標(Recovery Point Objective, RPO)。RPO一旦訂定完成，則可協助系統維護人員選擇適合的備份機制及頻率。如若訂定為1小時，則至少每小時必須進行一次資料備份，所選擇的儲存媒體可能為磁碟；但若RPO訂定為一週(168小時)，則至少每週進行一次資料備份，使用磁帶或光碟片等媒體即可滿足備份需求。	營運持續管理之資安程序 A-04-33-00-A2020	普	中	高	維運	由發展部定訂資訊服務失效之業務持續營運計劃。	確認發展部訂定之RPO。		
29			執行系統源碼與資料備份	應備份系統源碼與資料，備份時機如廠商交付或內容變更時，或依機關規定定期備份。	資訊系統資料備份作業 B-04-33-00-F1001	普	中	高	維運	以 NBU 排程實施備份。	由 DBA 提供備份記錄佐證資訊。		
30			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	常見之儲存媒體如磁碟、磁帶、光碟等，因使用方式及保存環境之差異，可能影響儲存媒體壽命而造成備份資料損毀。機關應訂定週期性測試時間表，並依時間表進行備份資料還原測試，以確保備份資料處於可用狀態。	資訊系統資料備份作業 B-04-33-00-F1001		中	高	維運	以 NBU 作業實施備份還原。	由 DBA 提供備份還原佐證資訊。		
31			應將備份還原，做為營運持續計畫測試之一部分	災害復原是營運持續計畫中相當重要之環節，其目的是為了在發生天災、人為疏失或惡意破壞造成資通系統損害時，能快速回復至正常或可接受的營運水準。營運持續計畫應定期完整測試、演練，以驗證計畫之適切性及有效性，在災害復原過程中應使用備份資料，以驗證備份機制是否正確可靠。	N.A.			高	維運				
32			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	備份資料應有適當的實體(如防火櫃等)及環境保護，且不可儲存於運作系統處，以避免因系統損毀造成無法取用備份資料之情況。將備份資料異地存放於離運作系統有一段距離之場所，則可減少災害(如火災等)發生時，同時傷害正式資料與備份資料的	N.A.			高	維運				
33		系統備援	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	機關應考量服務需求、使用現況、相關資源項目，以及資安事件發生之風險，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，亦可稱為復原時間目標(Recovery Time Objective, RTO)。	營運持續管理之資安程序 A-04-33-00-A2020		中	高	維運	由發展部定訂資訊服務失效之業務持續營運計劃。	確認發展部訂定之RTO。		
34			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	機關應準備適當及足夠的備援設備，或其他可提供服務的方式，以便在發生災害時，可於所訂定之容忍時間內讓服務回復正常運作。	營運持續管理之資安程序 A-04-33-00-A2020		中	高	維運	由發展部定訂資訊服務失效之業務持續營運計劃。	確認發展部有訂定資訊服務失效之取代服務。		
35	識別與鑑別	內部使用者之	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	資通系統應具備唯一識別及鑑別機關使用者之功能，如替內部使用者建立個別帳號，以強化系統之可歸責性(Accountability)。若多人共用同一個帳號登入系統，則難以從稽核紀錄識別確切的使用者身分。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	由開發廠商實作應用系統，每個系統帳號可識別唯一使用人員。	檢視系統使用者清單，確認沒有共用帳號。		

序號	構面	控制措施	安全需求項目	說明	本法人規範	普	中	高	類別	採取措施	驗證方式	驗證結果	備註
36	別	識別與鑑別	對資通系統之存取採取多重認證技術	系統身分驗證或重要交易行為，採用多重因素身分驗證以強化安全性。多重因素身分驗證係指具備兩種以上驗證類型，驗證類型一般區分為所知之事(如密碼、特定問題之答案)、所持之物(如晶片卡、憑證)及所具之形(如指紋、虹膜辨識等生物特徵)。	資訊服務帳號及密碼管理 B-04-33-00-B2040			高	技術	由開發廠商實作應用系統，雙因素認證。	檢查系統登入作業，是否符合本項要求		
37		身分驗證管理	使用預設密碼登入系統時，應於登入後要求立即變更	使用者註冊時係由資通系統或人工配發預設密碼者，於使用者首次登入時，應強制其變更預設密碼。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	由開發廠商實作應用系統，預訂密碼必須變更。	檢查系統登入作業，是否符合本項要求		
38			身分驗證相關資訊不以明文傳輸	身分驗證相關資訊不以明文傳輸。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	由開發廠商確認 MySQL 是以 SSL 機制通訊。	請系統開發者提供佐證資訊。		
39			具備帳戶鎖定機制，帳號登入進行身分驗證失敗達5次後，至少15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	系統應實作帳戶鎖定機制，並建議以電子郵件通知使用者。於鎖定期間禁止該帳號所有登入嘗試，超過鎖定時間則重新計次。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	由開發廠商實作應用系統，密碼錯誤鎖定機制。	檢查系統登入作業，是否符合本項要求		
40			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)	通行碼(密碼)的設定必須含有三類型字元組成，包含：英文字母、阿拉伯數字和特殊符號；長度不可少於八碼；通行碼(密碼)中不可包含使用者英文姓名、身份識別碼(ID)。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	由開發廠商實作應用系統，密碼複雜度。	檢查系統登入作業，是否符合本項要求		
41			上述兩點所定措施，對非內部使用者，可依機關自行規範辦理。	非內部使用者之身分驗證，可自行規範資通系統密碼複雜度、最短效期、最長效期，以及密碼歷程等限制。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	內外部密碼管制為一致的原則。	檢查系統登入作業，是否符合本項要求		
42			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)	使用者前3次舊密碼應被保留(以雜湊值形式)，於設定新密碼時，比對新密碼與舊密碼之雜湊值，若雜湊值相同則拒絕此次密碼設定。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	由開發廠商實作應用系統，密碼代數。	檢查系統登入作業，是否符合本項要求		
43			身分驗證機制應防範自動化程式之登入或密碼更換嘗試	系統若採用帳號密碼進行身分驗證，往往可能遭受到自動化程式以暴力破解方式嘗試登入。如圖形驗證碼(CAPTCHA)為常見的防範方式，透過將驗證碼以圖形方式呈現於頁面上，並要求使用者辨別該圖形中文字之方式，或以其他足以辨識人為動作之方式(如勾選特定選項等)，防堵自動化程式之嘗試行為。	資訊服務帳號及密碼管理 B-04-33-00-B2040			中	高	技術	由開發廠商實作應用系統，防制機器人登入。	檢查系統登入作業，是否符合本項要求		
44			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	密碼重設機制設計不良可能造成安全問題，常見錯誤是系統自行產生隨機密碼後以電子郵件寄送給使用者，此問題在於無法確保傳輸過程經過加密保護，故提高資安風險。使用者忘記密碼並啟動密碼重設機制時，應以使用者其他留存於系統的聯絡資訊，如電子郵件或手機號碼等，先要求使用者輸入該資訊，比對正確無誤後，發送一次性及具有時效性符記(如簡訊驗證碼、電子郵件驗證連結等)，一般會由亂數產生的英數字所組成，使用者接收後須於時效內進行輸入回傳動作，系統檢查回傳符記之有效性後，才允許使用者進行重設密碼動作。	資訊服務帳號及密碼管理 B-04-33-00-B2040			中	高	技術	由開發廠商實作應用系統，密碼重設機制。	檢查系統登入作業，是否符合本項要求		
45		鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊	資通系統身分鑑別頁面中，資料輸入欄位(如密碼等)應設定不以明文顯示方式，如以*取代真實輸入字元，以避免他人從旁窺視而盜取密碼。	資訊服務帳號及密碼管理 B-04-33-00-B2040	普	中	高	技術	由開發廠商實作應用系統，密碼不以明文呈現。	檢查系統登入作業，是否符合本項要求		

序號	構面	控制措施	安全需求項目	說明	本法人規範	普	中	高	類別	採取措施	驗證方式	驗證結果	備註
46		加密模組鑑別	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	密碼不可以明文方式儲存，應經過加密或雜湊處理，使得系統管理者或是惡意入侵的攻擊者皆無法輕易取得使用者原始密碼，以降低密碼外洩風險。實務上，當使用者設定密碼時，應針對該帳號產生一個亂數值(Salt)，將密碼結合亂數值，再以雜湊函式處理產生雜湊值後，分別於不同欄位儲存亂數值及雜湊值。後續使用者輸入密碼時，以輸入值添加當初設定密碼時產生的亂數，再次以雜湊函式處理，若產出結果同當初設定密碼時的雜湊值，則表示輸入密碼正確。	資訊服務帳號及密碼管理 B-04-33-00-B2040		中	高	技術	由開發廠商實作應用系統，密碼雜湊應再增加亂數值。	請系統開發者提供佐證資訊。		
47		非內部使用者之識別與鑑別	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)	資通系統若開放給外部使用者(含其他機關、委外開發與維護廠商、臨僱人員及一般民眾等)存取使用，應具備識別及鑑別之能力，如利用帳號、憑證或來源IP位址等方式，識別與鑑別使用者。	遠端連線服務管理規範 C-04-33-00-E1040	普	中	高	技術	維護廠商需電聯資訊室取得OTP登入主機，資訊室對登入人員留有紀錄。	抽察廠商維護之連線紀錄。		
48	系統與服務獲得	SDLC需求階段	針對系統安全需求(含機密性、可用性、完整性)進行確認	建議使用本表進行系統安全需求檢核。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	管理	依本表進行系統安全需求檢核。	依本表進行系統安全需求檢核。		
49		SDLC設計階段	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估	可參照「安全軟體設計參考指引」[3]之第3章安全軟體設計階段實務活動	應用系統開發及維運管理 B-04-33-00-D0001		中	高	管理	依系統功能需求實施風險評估。	由風評主責人員提供佐證資訊。		
50			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	系統發展生命週期需求階段發展之安全需求檢核項目，可能未能充分符合系統之所有安全需求，故應依據風險評估結果進行修正。	應用系統開發及維運管理 B-04-33-00-D0001		中	高	管理	依風險評估回饋結果，實施系統安全性改善。	改善項目: 捨棄PHP 重新改寫。		
51		SDLC開發階段	應針對安全需求實作必要控制措施	應於系統開發階段，針對安全需求實作必要之控制措施，輔以檢核表方式進行確認，可減少遺漏之可能。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	管理	依RFP及驗收條件管制。	檢視系統驗收項目是否有相關說明。		
52			應注意避免軟體常見漏洞及實作必要控制措施	軟體開發時應避免常見漏洞，如OWASP TOP 10[4]或CWE/SANS TOP 25[5]等，這些錯誤容易被惡意攻擊者利用，造成資料被竊取、竄改或使軟體無法運作，故需實作必要控制措施，以降低資安風險。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	管理	依RFP及驗收條件管制。	檢視系統驗收項目是否有相關說明。		
53			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	系統應設計錯誤處理機制，當系統發生錯誤時，儘可能採取錯誤代碼或簡短訊息呈現，避免將詳細或除錯用訊息直接顯示於使用者頁面，以防被攻擊者用來刺探系統內部資訊，或根據錯誤訊息推測出系統可能之弱點。確保系統所有功能的程式碼，在程式的進入點之後，盡可能採用程式語言的try-catch 陳述，捕捉可能發生的錯誤與例外狀況。另外，採用程式語言的finally陳述，確保將該段功能程式碼所使用的資源正確釋放。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	技術	依RFP及驗收條件管制。	實機測試異常訊息，是否符合保護原則。		
54			執行「源碼掃描」安全檢測	源碼檢測可於程式開發及測試階段進行，以及早發現源碼之安全實作問題，並進行修補。	應用系統開發及維運管理 B-04-33-00-D0001			高	管理	源碼掃描作業。	由源掃主責人員提供佐證資訊。		
55			系統應具備發生嚴重錯誤之通知機制	系統應區分錯誤等級，若發生嚴重等級錯誤時，採用電子郵件或簡訊等通知機制，使系統管理員或相關人員可及時掌握狀況，以利進行後續處理。	應用系統開發及維運管理 B-04-33-00-D0001			高	技術	依RFP及驗收條件管制。	實機測試，不同等級之異常警示作業。		
56		SDLC測試階段	執行「弱點掃描」安全檢測	弱點掃描係利用自動化工具，對受測目標進行安全性掃描，以找出系統潛在弱點。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	管理	弱點掃描作業。	由弱掃主責人員提供佐證資訊。		
57			執行「滲透測試」安全檢測	滲透測試係在取得合法授權後，對受測目標進行安全探測，由專業人士模擬駭客的攻擊行為，以人工及自動化掃描工具或攻擊程式等方式，尋找並利用系統弱點入侵系統，並於檢測作業完畢後提供完整的評估報告。	應用系統開發及維運管理 B-04-33-00-D0001			高	管理	滲透測試作業。	未編列相關預算，故本項無法檢核。		

序號	構面	控制措施	安全需求項目	說明	本法人規範	普	中	高	類別	採取措施	驗證方式	驗證結果	備註
58		SDLC部署與維運階段	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	就作業系統或平台之安全更新，定期評估、測試與更新。系統上線前，就作業系統或平台預設開啟的服務與埠口(Port)進行檢視與評估，正面表列需要開啟該服務及埠口之理由，並關閉不必要之項目。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	管理	以防火強管制服務port。	由FW管理者提供佐證資訊。		
59			資通系統不使用預設密碼	系統相關軟體元件或組態設定若有使用預設密碼，應於系統正式上線前變更完畢。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	技術	依系統組態或架構圖檢視包含出廠或預設密之元件。	本系統架構中，未包含有出廠或預設密之元件。		
60			於系統發展生命週期之維運階段，應執行版本控制與變更管理	應具備版次世代(至少5代)管理，在維運階段可能因需求變更、系統除錯、功能精進等原因而需要變更系統組態，而版本控制之目的，即在記錄系統組態在某段時間內的變更行為，使得使用者在需要時可取回特定的版本，嚴謹的版本控制與變更管理可強化系統的安全性與可用性。	應用系統開發及維運管理 B-04-33-00-D0001		中	高	維運	應有版本管控作業。	應有版本管控作業。		
61		SDLC委外階段	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	機關委外開發資通系統時，可參考本文件之內容，並依據不同之安全等級(高、中、普)制定適用之安全需求，明確納入委外契約以做為驗收時之依據。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	維運	RFP。	委外合約是否包含相關資安條款。 是否執行。		
62		獲得程序	開發、測試以及正式作業環境應為區隔	開發環境、測試環境與正式作業環境可區隔成不同的設備及網段，限制所能存取的應用程式及資料庫，以保護正式作業環境系統及資料。實務上，開發人員常以本機電腦為開發環境，並連結使用本機端之資料庫進行應用程式開發。俟開發完畢則將應用程式部署至測試主機，並連結至測試用資料庫，供測試人員進行測試使用。俟測試完畢，再將應用程式部署至正式環境，並連結至正式資料庫提供上線服務。	應用系統開發及維運管理 B-04-33-00-D0001		中	高	維運	依系統架構應區分開發區、測試區、正式區。	系統架構是否區分開發區、測試區、正式區。		
63		系統文件	應儲存與管理系統發展生命週期之相關文件	系統發展生命週期之相關文件如系統需求書、系統規格書、系統發展計畫、系統測試計畫及測試報告等，應書面或電子化形式進行文件保存，並被納入管理程序。	應用系統開發及維運管理 B-04-33-00-D0001	普	中	高	維運	委外系統開發及驗收文件。	委外系統開發及驗收文件。		
64	系統與通訊保護	傳輸之機密性與完整性	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	資訊系統傳輸機敏資料時，應避免明文傳輸。實務上，常採用加密傳輸協定(如HTTPS等)，以確保機敏資料傳輸過程中的安全，並應採取較安全的傳輸協定(如TLS1.2以上)及加密演算法(Cipher)，以降低被破解之風險。亦可進一步於伺服器端設定強制使用加密傳輸協定(如啟用網站安全性標頭之HTTP Strict Transport Security強制安全傳輸技術等)，避免使用者透過非加密傳輸協定存取應用系統伺服器。	網路管理規範 B-04-33-00-B1012			高	技術	門諾公益捐款網站, 僅能以 https 運作。	驗證捐款網站憑證效期。		
65			使用公開、國際機構驗證且未遭破解之演算法	方式且未經過適當的驗證程序，可能存在設計瑕疵，增加被破解的風險。應採用公開、國際認可之演算法，如AES對稱式加密演算法、RSA非對稱式演算法及SHA安全雜湊演算法等。	網路管理規範 B-04-33-00-B1012			高	技術	門諾公益捐款網站, 僅能以 https 運作。	驗證捐款網站憑證效期。		
66			支援演算法最大長度金鑰	系統若採用密碼學演算法時，應使用該演算法目前支援的最大金鑰長度，以減少被暴力破解解密之可能及弱點。	網路管理規範 B-04-33-00-B1012			高	技術	門諾公益捐款網站, 僅能以 https 運作。	驗證捐款網站憑證效期。		
67			加密金鑰或憑證應定期更換	產生網站HTTPS使用之憑證，應具備使用年限限制，並於到期前進行更換。系統若另行使用自行產生之加密金鑰，亦需定期更換。	網路管理規範 B-04-33-00-B1012			高	管理	門諾公益捐款網站, 僅能以 https 運作。	驗證捐款網站憑證效期。		
68			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	伺服器端之金鑰一旦外洩，則加密機制視同無效，嚴重危害系統之機密性，故應訂定相關作業標準或管理規範，以妥善保護金鑰。如不將加密金鑰與加密資料存放於同一系統中，或對於加密金鑰的存取進行限制。	網路管理規範 B-04-33-00-B1012			高	維運	IIS網站憑證以 OS層註冊，為其保護機制。	請 IIS 管理者提供佐證資訊。		
69		資料儲存之安全	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	參數設定或系統設定存放處，應限制存取及進行加密。	應用系統開發及維運管理 B-04-33-00-D0001			高	技術	由開發廠商實作應用系統，密碼雜湊應再增加亂數值。	請系統開發者提供佐證資訊。		

SSDLC採取措施及驗證查核表

序號	構面	控制措施	安全需求項目	說明	本法人規範	普	中	高	類別	採取措施	驗證方式	驗證結果	備註
70	系統與資訊完整性	漏洞修復	系統之漏洞修復應測試有效性及潛在影響，並定期更新	針對系統所使用的外部元件與軟體進行表列，包含其版本資訊，定期關注元件版本更新訊息及安全漏洞通告，若有相關之安全漏洞，評估系統元件更新之必要性，並於系統測試環境進行更新測試驗證後，才於正式環境進行更新。	電腦設備及軟體管理規範 B-04-33-00-B1011	普	中	高	管理	依GCP 定期派送微軟更新作業。	檢視主機為最近之更新。		
71			定期確認資通系統相關漏洞修復之狀態	注意相關之安全漏洞訊息(透過CVE 相關訊息網站、廠商安全通告等)，若發現採用之軟體或元件具有安全漏洞，應設法修復漏洞並定期追蹤修復之狀態。	電腦設備及軟體管理規範 B-04-33-00-B1011		中	高	維運	依GCP 定期派送微軟更新作業。	檢視主機為最近之更新。		
72		資通系統監控	發現資通系統有被入侵跡象時，應通報機關特定人員	應指派人員負責處理資通系統入侵攻擊相關資安事件，並於發現資通系統有被入侵跡象時，通報相關人員進行處理。	資訊安全事故管理 B-04-33-00-B1026	普	中	高	維運	依資安事件通報規範處理。	檢視系統事件是否有依通報規範處理。		
73			監控資通系統，以偵測攻擊和未授權之連線，並識別資通系統之未授權使用	應指派人員負責處理資通系統入侵攻擊相關資安事件，並於發現資通系統有被入侵跡象時，通報相關人員進行處理。	資訊專案管理 C-04-33-00-C1020 網站維護合約		中	高	維運	RFP 要求定期檢視系統是有異常檔案。	檢視合約是否有要求定期檢視系統異常檔案。		
74			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	機關應透過多種工具及技術(如入侵偵測系統、入侵防禦系統、WEB應用程式防火牆、網路設備流量監控軟體等)達成監控能力，監控資通系統所有進出之通訊活動，以發現不尋常或未經授權之連線及存取行為，並進行資安事件分析。	網路管理規範 B-04-33-00-B1012			高	維運	將捐款網站納入WAF內控管。	由WAF管理者提供佐證資訊。		
75		軟體及資訊完整性	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊	提供完整性驗證工具以驗證軟體或資訊在儲存或傳輸過程中未被人惡意竄改，如網站可在檔案下載連結處，提供以安全雜湊演算法產生之雜湊值，並說明使用的雜湊演算法為何，供使用者取得資料後自行計算雜湊值進行比對。另外，為確保系統程式之完整性，可對系統程式檔案留存雜湊值，並進行監控比對，以偵測未授權之惡意變更。	電腦設備及軟體管理規範 B-04-33-00-B1011		中	高	技術	導入目錄檔案監控工具。	導入目錄檔案監控工具。		
76			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應檢查是否符合預期之邏輯規則，實務上，以正規表示式(Regular Expression)驗證內容之合法性。檢查機制若於客戶端實作，容易被使用者繞過檢查機制，故應於應用系統伺服器端實作始視為有效。	應用系統開發及維運管理 B-04-33-00-D0001		中	高	技術	由開發廠商實作應用系統，使用者輸入應於伺服器端檢查。	請系統開發者提供佐證資訊。		
77			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	機關應訂定相關安全保護措施，在發現資通系統完整性遭到破壞時採取適當之行動。如當發現資料庫或檔案被不當竄改、站台被植入惡意指令碼或元件等資安事件時，應通知系統管理者進行緊急應變處置，並依規定之通報流程進行資安事件通報作業。	資訊安全事故管理 B-04-33-00-B1026 資訊安全矯正及改善程序書 B-04-33-00-B1027			中	高	維運	依資安事件通報規範及改善程序處理。	檢視系統事件是否有依通報規範處理及緊急應變處置。		
78			應定期執行軟體和資訊完整性檢查	重要資料或紀錄，以安全雜湊演算法產生並留存其雜湊值，後續可對資料再次產生雜湊值並與原先結果進行比對，以確保資料未遭異動竄改。	N.A.			高	管理				