New eID 系統相關安全性做法

壹、共通規範：

一、 依照資通安全管理法及其子法、「資通安全事件通報及應變辦法」及本部「資通安全與個資事件通報及應變管理程序」規範，明確訂定各單位及委外供應商資安事件通報及應變流程與時限。

二、 遵循內政部資訊系統委外服務案資訊安全管理規範(參考附錄一)，並要求廠商應遵循與配合下列面向之要求：

(一) 存取控制要求。

(二) 運作安全要求。

(三) 通訊安全要求。

(四) 密碼措施安全要求。

(五) 系統取得、開發及維護安全要求。

(六) 供應商關係安全要求。

(七) 資訊安全事故管理安全要求。

三、 依「系統安全需求項目查檢表」(參考附錄二)作下列分類的相關檢查項目：

(一) 機密性。

(二) 完整性。

(三) 可用性。

(四) 身分驗證。

(五) 授權與存取控制。

(六) 日誌紀錄。

(七) 會談（Session）管理。

(八) 錯誤及例外管理。

(九) 組態管理。

貳、建置期：

一、 策略面

(一) 透過獨立驗證團隊(IV&V)及資安稽核團隊（如行政院國家資通安全會報技術服務中心），監督所有的建置作業均符合契約規定及 ISMS/PIMS 的安全標準規範（如 ISO27001、ISO27701、BS10012 等）。

(二) 規劃 110 年 1 月擇定部分縣市採民眾自願申請之方式進行半年的小規模發行，並辦理賞金獵人活動，同時開放民間團體進行黑箱測試，確保資安無虞後，再全面啟動換證作業。

二、 管理面

(一) 安全管理措施

1、設備安全：委外廠商人員所須存取之資料或攜入之資訊設備，包括個人電腦、

平板電腦、行動電話、智慧卡及所有形式的儲存設備等，於機關場所內使用任何資訊處理設備均應受管理。

2、門禁管理：委外作業人員進出工作場所，均應配帶員工證件，非經許可不得至工作場所以外地區活動，且須由本機關人員陪同作業。

3、供應鏈管理：

A.資訊委外廠商人員需簽署保密切結文件，人員資格須經過審核才可擔任。(參考附錄三)

B.資通安全機制監督與稽核（含帳號權限審核紀錄、存取紀錄資料之稽核）。

C.特殊機敏資料存取授權（含職責分工(separation of duty)、多人控管(dual control)、限制行動化裝置使用、對外網路連線過濾等）。

4、晶片卡片：卡片提供廠商需佐證相關製作流程具有備援機制，確保主/備援晶片均能滿足功能需求，且具有長期供應的能力，定期召開安全檢視會議，以評估各晶片是否安全或需要更換。

5、資訊系統：於可控之安全場地進行開發環境測試與建置，包含整合式開發環境（IDE）、軟體開發套件（SDK）等。

(二) New eID 系統建置規劃同地及異地備援機制，確保風險發生時服務不中斷。

(三) 建置「授權驗證系統」，控管需用機關讀取 New eID 之加密區資料，需用機關除須取得民眾同意且須輸入密碼（PIN1）外，尚須取得本部審查授權需用機關依其執行法定業務所需後簽發之憑證，以 Secure API 讀取加密區資料，以保護民眾相關隱私。

(四) 研議需用機關開發應用系統應遵循之 New eID 資料驗證安全檢查表（暫定），供需用機關作為系統安全檢查之依據。

三、 技術面

(一) 應用程式開發應遵循安全系統發展生命週期（SSDLC），於系統開發各階段納入安全評估與安全措施，確保系統安全。

(二) 應於封閉網路進行應用程式開發、維運及管理作業。

(三) 應用系統、資料庫及網域主機密碼應符合長度與複雜度原則，且勿使用弱密碼及鍵盤順序。

(四) 開發環境其程式原始碼之存取權限應予控管（含版本控制、源碼檢測、佈署管理等）。

(五) 系統設計應採取個資最小化原則。

(六) 建立資安弱點通報機制，得以即時辨識系統軟硬體可能之資安弱點。

(七) 應用程式上線前或功能變更時，須進行相關風險評估與技術檢測（源碼檢測、弱點掃描）。

(八) 將系統建置於內政資料中心之內網環境中，對外連線系統採用虛擬專用網路（VPN），並設有防火牆入侵偵測及防護機制，確保資料通訊安全。

(九) 依據「內政部憑證管理中心憑證作業基準」規範，晶片金鑰對須於晶片中自行運算產生，確保私密金鑰無法匯出、重製。

參、維運期：

一、 完善的權限控管機制。

二、 異常行為監控及紀錄

依據「政府機關（構）資通安全責任等級分級辦法 A 級之公務機關應辦事項」規定辦理下列事宜：

(一) 針對資訊系統定期辦理網站弱點掃描、滲透測試及資安健診等安全性檢測；資安責任等級「高」之資訊系統須辦理源碼檢測事宜。

(二) 建立資安防禦縱深，部署 IDS/IPS、WAF 應用程式防火牆、郵件過濾裝置、防毒軟體及進階持續性威脅攻擊防禦措施等資通安全防護事宜。

(三) 應針對正式區域伺服器、各式主機佈署應用程式白名單機制，並檢驗確認可僅允許經過授權之程式執行，阻擋不在白名單之內的應用程式，並且當未經授權程式嘗試執行時通報資安監控中心或是其他中控管理系統。

(四) 建立資訊安全監控中心(SOC)，執行 7*24 小時惡意活動偵測、監控及通報，即時掌握網路威脅，快速回應資安事件。

(五) 辦理資通安全教育訓練，提升同仁資安防護意識，提高資安警覺性。

三、 定期檢視作業系統日誌及網站日誌，並依資通安全管理法及本部資訊安全管理制度(ISMS)規定辦理日誌之管理與保存作業。

四、 針對作業系統、系統開發元件應定期檢視是否存在資安漏洞並進行修補事宜。

五、 政府組態基準(GCB)：依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。

六、 定期的內外部資安稽核

(一) 依據「政府機關（構）資訊安全責任等級分級作業施行計畫」規範中定義，除希望政府機關能遵守行政院及所屬各機關資訊安全管理規範外，各機關應依其不同資安等級規劃稽核方式如下：

1、A 級單位每年至少執行 2 次內部稽核。

2、B 級單位每年至少執行 1 次內部稽核。

3、C 與 D 級單位得執行自我檢視。

(二) 內外部資安稽核

資安稽核	項目
內部資安稽核	針對業務應用系統、應用程式（含 API 及 APP）與資料庫保留詳細操作紀錄並提供資安稽核機制。
	針對系統帳號之行為進行記錄，並進行分析，確保無高風險之操作行為，並通知系統管理者。
	系統針對系統管理者及使用者之操作行為進行紀錄，並根據頻率及規則分析，確保無高風險之操作行為。
	應用程式（含 API 及 APP）與資料庫應能針對使用者之操作行為進行記錄，可與登入應用程式帳號關聯，並根據數值、命令、時間、地點、頻率等行為訂立規則分析，確保無高風

	險之操作行為。
外部資安稽核	業務應用系統應記錄使用者之登入與登出之行為，分析出異常行為並通知該帳號擁有者。
	業務應用系統應記錄使用者登入失敗之行為，分析出異常行為並通知管理者與該帳號擁有者。
	業務應用系統應紀錄系統事件並分析異常使用行為。

內政部資訊系統委外服務案資訊安全管理規範

一、 廠商應遵循內政部(以下簡稱本部)資訊安全管理制度等相關規範，強化資訊安全管理，以確保資料傳送、儲存及流通之安全。

二、 廠商應遵循與配合下列存取控制要求：

（一） 禁止使用未經授權之網路設備及線路連結內部網路；如協助處理機密等級及限閱等級資料，應考量業務需求及資源可行性，決定是否採用專屬（隔離）之網路作業環境。

（二） 避免使用共用帳號，如有特殊需求，須經機關之權責主管同意；因業務與資訊作業需求而使用資通訊設備或有帳號及權限異動需求者，應透過「帳號新增/異動申請表」進行申請及審核；如有因作業需求而持有系統管理員帳號，廠商應配合機關系統管理人員採取適當審核及確認作業。

三、 廠商應遵循及配合下列運作安全要求：

（一） 伺服器作業系統更新前，廠商應協助評估更新作業對應用系統之影響，或於測試環境測試無誤後再行申請更新作業；廠商進行開發、測試及線上運作之環境應設置於不同網路區段或資訊處理設施，以降低線上運作環境遭未經授權存取或變更之風險。

（二） 廠商如需使用外來可攜式設備或媒體，應確認未遭受病毒感染。

（三） 廠商應建立系統技術脆弱性資訊之取得管道，評估可能帶來之風險，並確認系統修正或安全問題更新程式之影響與處理方式。

（四） 廠商應定期配合執行弱點掃描作業。

（五） 系統須建置將使用者異動情形紀錄於稽核日誌之功能，且系統應提供查詢系統帳號之建立、修改、啟用、禁用及刪除動作、授予權限功能及異動紀錄。

（六） 資訊系統應就涉及機敏資料部分建立稽核日誌,並確保資訊系統有稽核特定事件(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）之功能，且僅限特定授權之使用者存取稽核日誌。

（七） 稽核日誌需具備以下項目：

1. 識別使用者之 ID，不可為個人資料類型。

2. 時間應紀錄至秒等級。

3. 執行功能或存取資源名稱。

4. 執行結果或事件描述。

5. 網路來源及目的位址。

（八） 應用系統主機須建立時間同步機制。

四、 廠商應遵循與配合下列通訊安全要求：

（一） 若攜帶電腦或網路設備至本部，未經核准不得接入本部網路；禁止使用未經授權之網路設備、線路及私人電腦等設備連接內部區域網路。

（二） 如有連線作業，須透過安全閘道（如：防火牆）或相關網路設備進行管控。

（三） 未經許可不得以任何儀器設備或軟體工具進行網路通訊側錄、檢測及掃描；主機與網路設備連結之網路線不可隨意插拔、更換或接上其他非經允許使用之設備。

（四） 如有常態性或定期資訊傳送作業，應述明交換內容、使用目的、範圍、風險控管等項目，經核可後始能辦理。

（五） 執行電子傳輸前，機關及廠商須簽定保密協議文件，並依資訊機敏程度協議適當傳輸方式及安全保護措施(如：採行帳號密碼管制、電子資料加密或電子簽章認證等)；如透過網際網路傳送機敏資料，應使用安全性連線方式傳輸（如：SFTP 及 HTTPS）或經由虛擬專用網路（VPN）處理，以確保資料隱密性；如透過專線傳送（如：封閉網路系統）機敏資料，應依資料安全等級，依相關安全規定適當加密處理。

（六） 系統如有機敏資料存於資料庫或其他儲存媒體時，需採用對稱式或其他加密方式，將機敏資料加密成密文後儲存；傳輸機敏資料時，採用 HTTPS 等加密協定，確保機敏資料以密文方式傳輸。

五、 廠商應遵循與配合下列密碼措施安全要求：

（一） 廠商若使用憑證應用服務對訊息機密性、完整性、不可否認性、與可使用性之安全管控要求，應依據電子簽章法及其施行細則規劃與建置適當之亂碼化安全控管機制。

（二） 系統加密方式，應採用公開、國際機構建議安全且未遭破解之演算法（如 AES 對稱式加密、RSA 非對稱式及 SHA-2 安全雜湊等演算法），並使用該演算法支援之最大金鑰長度，以減少被暴力破解解密之可能及弱點。

六、 廠商應遵循及配合下列系統取得、開發及維護安全要求：

（一） 廠商應參考現有系統或作業文件以進行應用系統開發、變更、增修需求之確認，瞭解現行作業流程，利用分析所收集到之資料，進行可行性與技術、作業執行及應用效益之評估，並應考量對現有資訊環境之影響。

（二） 廠商應依據系統特性，規劃系統程式備份作業，並依據運作安全管理程序定期執行及驗證備份資料。

（三） 廠商執行應用系統開發及維護之各階段活動時，宜參考「應用系統文件內容檢核表」產製相關文件。

（四） 系統開發、變更及增修，應於需求分析階段即將資訊安全需求納入，並考量下列系統安全設計原則：

1. 系統應具備登入身分驗證機制，系統登入安全管理應參考存取安全管理程序設計。

2. 系統之設計應確保輸入與輸出資料、系統內部處理程序、系統與系統間資料介接、及系統紀錄訊息之資料完整性。

（五） 對於字串之輸入應加以過濾或檢查，並限制前端應用程式資料輸入之長度及型別，並針對各輸入資料項目，規劃下列資料驗證功能：

1. 是否超出輸入資料之設定範圍。

2. 是否有錯漏之文字或數字。

3. 是否有資料毀損或不正確。

4. 是否有未經授權之資料或不一致之控制性資料。

5. 過濾如「 ';"-- @ %」之類非預期之輸入字元。

（六） 資料欄位之輸入為已知之資料範圍，應提供選單或選項之方式提供使用者輸入。

（七） 有關機敏資料之輸入，應使用適當之遮罩或隱碼措施。

（八） 系統應考量業務需求特性，設計使用者登入或連線逾時自動登出（以 15 分鐘以內為原則）或工作階段逾時（Session timeout）功能。

（九） 應用程式應設計各種例外狀況管理（擷取和回傳例外狀況、設計例外狀況案例、傳送例外狀況資訊等）及處理機制，以利擷取及存錄錯誤資訊；並防止直接顯示原始完整錯誤訊息於終端使用者畫面。

（十） 應用程式執行檔與暫存檔及其目錄應採取適當檔案保護措施(如:加密或存取限制)。

（十一）系統應考量資料重要性，針對重要功能作業（例如：登入、登出、資料刪除或變更等）留存軌跡紀錄。

（十二）機敏資料應在傳輸及儲存過程加密保護，並定期檢討加密機制之有效性。

（十三）應用系統開發及測試環境，應與正式線上環境區隔。

（十四）程式撰寫時應考量安全問題，避免出現已知弱點。

（十五）軟體開發生命週期中，考量開發方法之安全性，且建立使用各程式語言之安全開發指南。

（十六）系統開發完成後應進行測試，除測試系統功能外，亦應測試系統安全性。

（十七）開發人員應具備安全開發知識或接受相關訓練，以具備可避免、發現和修復脆弱性之能力。

（十八）若需轉移開發資料，應有適當安全傳輸機制。

（十九）廠商應進行程式碼安全檢測或程式碼檢視。

（二十）確認程式碼無論是新開發或變更，已由原始程式碼作者以外熟知程式碼檢查技術和安全程式碼實務之人員，參考業界安全程式碼標準檢視完竣。

（二十一） 應用系統整合測試階段，應通過程式碼安全檢測（源碼掃描）或應用系統安全性檢測，並透過執行弱點掃描、滲透測試（黑箱測試）或應用程式安全掃描（白箱測試），檢查程式碼之安全性並修復至通過檢測。

（二十二） 變更前需先進行必要之資料備份，以確保系統變更作業不致影響或破壞系統原有安全控制措施，以及變更失敗時可執行還原作業。

（二十三） 廠商交付之系統，不得包含任何後門程式、隱密通道及特洛伊木馬程式等。

（二十四） 系統須加強輸入檢核以防止 SQL Injection、XSS、篡改輸入等攻擊，並配合機關要求，在必要時協助建立 SQL Injection 與異常行為分析功能與報表；對於使用者輸入欄位資料，採用正規表示式（Regular Expression）進行檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法。

（二十五） 系統需符合 IPV4 及 IPV6 協定。

（二十六） 網站系統若具有與其他外部系統或資料庫之連線需求，不可將連線之身分驗證資訊（帳號、密碼等）寫於程式原始碼中，應採用設定檔或於系統啟動時動態輸入之方式。如以參數方式留存於設定檔，應確認僅有執行該系統之作業系統帳號可以存取設定檔。

（二十七） 系統除了允許匿名存取之功能外，所有功能都必須已通過身分驗證才允許存取。網站除公開區域外，其他網頁皆需進行身分驗證登入成功後，才得以存取。系

統傳遞身分驗證相關資訊（如：帳號、密碼等）應採用加密傳輸，不以明文傳輸，以避免資訊被攔截或監聽竊取。

七、 廠商應遵循與配合下列供應商關係安全要求：

（一） 廠商及其分包商於委外契約簽訂時，應與機關簽訂相關保密文件。

（二） 廠商存取本部資訊處理設施或資訊時，應遵循法規與本部資訊安全管理制度，審慎評估其風險，採取適當控制措施。

（三） 廠商若有下包廠商時，應要求其下包廠商亦應遵循本部資訊安全管理要求，必要時機關應審查廠商要求下包廠商之佐證資訊或文件。

（四） 廠商所提供之服務若發生錯誤、中斷或資安事件，應留存相關紀錄，必要時機關應進行調查或稽核。

（五） 廠商應配合機關資訊安全工作小組稽核分組不定期稽核資訊安全管理作業，或審查有關資訊安全之第三方外部稽核報告。

（六） 廠商應配合機關專案承辦人員定期檢視與審查服務內容、報告及紀錄，以確保所提供之服務符合雙方協議同意等級。

八、 廠商應遵循與配合下列資訊安全事故管理安全要求：

（一） 廠商發現疑似資訊安全或個資外洩等異常事件或事故時，應負有即時通報機關資訊安全工作小組或個人資料保護管理小組，並提供事件或事故相關資訊之責任。

（二） 廠商發現可疑之資訊安全事件、事故或安全弱點時（如：人員發現電腦使用異常情形、應用系統異常狀況告警、資訊機房管理人員發覺硬體設施、伺服器等設備發生異常狀況等）、或個人資料侵害告警事件或事故時，應立即以口頭、電話等方式通知本部資訊中心，本部資訊中心人員初判非屬一般維修情形，而為資訊安全/個人資料事件或事故後，應通報至事故通報處理分組。

系統安全需求項目查檢表

項次	分類	檢查項目	說明
1	1.機密性	1.1 機敏資料傳輸時，採用加密機制	說明：網站傳輸機敏資料時，採用 HTTPS（透過 TLS 等加密協定）協定以確保機敏資料以密文方式傳輸。
2		1.2 使用公開、國際機構驗證且未遭破解的演算法	說明：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 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。
3		1.3 使用演算法支援的最大長度金鑰	說明：系統中採用密碼學演算法時，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。例如 AES256bits、RSA2048bits 或以上、SHA-512 等。
4		1.4 加密金鑰或憑證週期性更換	說明：產生網站 HTTPS 使用之憑證，應具備 3 年以下之使用年限限制，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。
5		1.5 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	說明：常見加密金鑰以檔案形式放置於作業系統中，並以路徑存取，此作法之安全性較採用獨立之硬體安全模組（hardware security module，HSM）來保護金鑰為低。採用獨立之硬體安全模組，通常將金鑰保護於硬體晶片環境以避免被竊取，同時具備多種驗證類型（IP、PIN 碼等），對金鑰存取進行限制。（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）
6		1.6 機敏資料儲存時，採用加密機制	說明：機敏資料存於資料庫或其他儲存媒體時，採用對稱式或其他加密方式，將機敏資料加密成密文後儲存，並於需要取得原文明文時解密還原。此作法可減少機敏資料因儲存媒體有其他存取管道而洩漏的風險。

項次	分類	檢查項目	說明
7	2.完整性	2.1 於伺服器端以正規表示式（RegularExpression）方式，檢查使用者輸入資料合法性	說明：對於使用者輸入欄位資料，於伺服器端採用正規表示式（RegularExpression）進行檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法。
8		2.2 針對開放下載的資料，也提供資料之雜湊值（HASHValue）供使用者比對其完整性	說明：網站提供使用者下載的資料，於下載連結處，以安全雜湊演算法產生雜湊值（HASHValue）供使用者參考比對，並說明使用的雜湊演算法為何。
9		2.3 具有防範 SQL 命令注入攻擊（SQLInjection）之措施	說明：系統於伺服器端具有防範 SQL 命令注入攻擊措施。例如，Preparedstatements、Storedprocedures、輸入驗證（InputValidation）等。
10		2.4 具有防範跨站腳本攻擊（Cross-SiteScripting）之措施	說明：系統於伺服器端具有防範跨站腳本攻擊（Cross-SiteScripting）措施。例如黑名單過濾跳脫特殊字元、白名單正規表示式驗證、輸出編碼等。此安全需求項目僅適用於 WEB 網站系統。
11		2.5 驗證網頁重導（Redirects）與導向（Forwards）之目的地在合法名單內	說明：網站若提供網頁重導或導向之功能，必須確認使用者輸入欲重導向的網頁，其值在合法白名單內，以避免被利用來重導向至惡意網頁。此安全需求項目僅適用於 WEB 網站系統。
12		2.6 重要系統資料或紀錄留存雜湊值以確保完整性	說明：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，以確保資料未遭到異動竄改。
13	3.可用性	3.1 重要資料定時同步至備份或備援環境，並加以保護限制存取	說明：系統具備重要資料定時備份機制，依組織規範將資料同步至備份或備援環境，以避免系統毀損或資料綁架勒索對資料可用性之危害。重要資料於備份或備援環境應有保護限制存取措施，以避免增加其他資安風險。
14		3.2 採用「高可用性」（HighAvailability）架構（分散式或叢集伺服器架構）	說明：系統之服務水準，經評估後須滿足高可用性需求者，應考量採取分散式或叢集伺服器架構，以使當系統發生錯誤情況

項次	分類	檢查項目	說明
			或硬體毀損時，服務仍能正常運作。
15	4.身分驗證	4.1 除了允許匿名存取的功能外，所有功能都必須已通過身分驗證才允許存取	說明：網站除公開區域外，其他網頁皆需已進行身分驗證登入成功後，才得以存取（接續應檢查該使用者權限是否允許其存取該網頁或功能）。使用者若存取非公開區域，檢查機制發現其尚未通過身分驗證時，應不允許其存取頁面並將其導向至首頁或登入頁面。
16		4.2 身分驗證機制位於伺服器端且採用集中過濾機制（例如使用 Filter 過濾器）	說明：系統應包含具有一致全面性、位於伺服器端，強制適用於全系統的授權及存取控制機制。例如使用 Filter 過濾器機制。
17		4.3 身分驗證相關資訊（帳號、密碼等）不留存於程式原始碼中	說明：網站系統若具有與其他外部系統或資料庫等連線的需求，不可將連線之身分驗證資訊（帳號、密碼等）寫於程式原始碼中，應採用設定檔或於系統啟動時動態輸入之方式。身分驗證資訊若以參數方式留存於設定檔，應確認僅有執行該系統之作業系統帳號可以存取設定檔。
18		4.4 確實規範使用者密碼強度（密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元）	說明：若採用密碼作為身分驗證機制，當使用者設定密碼時，需以正規表示式檢查密碼強度是否符合標準，例如密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元。
19		4.5 使用者必須定期更換密碼，且至少不可以與前 5 次使用過之密碼相同	說明：使用者初次設定或異動密碼時，系統應留存設定密碼之時間，往後每次使用者成功登入後，必須檢查該組密碼是否已使用超過組織政策所規定的最長期限（例如，45 天），若已超過時限則強制使用者更換密碼，使用者的前 5 次舊密碼應被保留（以雜湊值的形式），新密碼應比對且不允許與前次使用密碼相同。

項次	分類	檢查項目	說明
20		4.6 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 3 次後，至少 30 分鐘內不允許該帳號及來源 IP 繼續嘗試登入	說明：系統須具備帳戶鎖定機制，紀錄使用者身分驗證錯誤次數，若錯誤次數達到組織資安規範之次數（例如，3 次），則針對該帳號及來源 IP 進行鎖定一段時間（例如，30 分鐘）。鎖定時間後使用者再次進行身分驗證登入嘗試時，應將錯誤次數歸零。除帳號外亦鎖定來源 IP 的用意為防範攻擊多個帳號，使同一來源無法在某個帳戶鎖定後，又再行嘗試其他帳戶。
21		4.7 身分驗證相關資訊不以明文傳輸	說明：系統傳遞身分驗證相關資訊（例如帳號密碼）時，採用加密傳輸，以避免該資訊被攔截或監聽竊取。
22		4.8 密碼添加亂數（Salt）進行雜湊函式（HASHFunction）處理後，分別儲存亂數及雜湊後密碼	說明：系統儲存使用者密碼時，不宜儲存明文密碼，以避免遭到有心人士竊取。使用者設定密碼時，應針對該使用者產生一個亂數值，將使用者密碼結合亂數值，再以雜湊函式（HASHFunction）處理產生雜湊值後，分別於不同欄位儲存使用者亂數值及雜湊值。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。
23		4.9 採用圖形驗證碼（CAPTCHA）機制於身分驗證及重要交易行為，以防範自動化程式之嘗試	說明：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。另外，系統重要行為若被獲知相關執行參數，亦可能被自動化程式嘗試偽冒合法使用者觸發。因此，採用圖形方式顯示一驗證碼於頁面上，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（例如勾選特定選項），將可以防堵自動化程式之嘗試行為。
24		4.10 重要交易行為要求使用者再次進行身分驗證	說明：系統中重要交易行為，於執行前應再次確認獲得授權。要求使用者再次身分驗證是確認獲得授權的手段之一。另外此作法亦可有效防堵攻擊者透過其他方式

項次	分類	檢查項目	說明
			取得使用者身分憑證後，直接偽冒使用者執行重要交易行為。
25		4.11 採用多重因素身分驗證（兩種以上驗證類型）	說明：系統身分驗證或重要交易行為，可採用多重因素身分驗證以強化安全性。多重因素身分驗證意指具備兩種以上驗證類型，驗證類型一般區分為所知之事（Somethingyouknow）、所持之物（Somethingyouhave）及所具之形（Somethingyouare）。所知之事類型常採用密碼、特定問題之答案等。所持之物類型常採用令牌（Token）、憑證、簡訊、電子郵件等。所具之形類型常採用生物特徵，如指紋、虹膜辨識等。
26		4.12 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令牌（Token），檢查傳回令牌有效性後，才允許使用者進行重設密碼動作	說明：密碼重設機制設計不良可能造成安全問題。常見錯誤是系統主動將密碼重新設定後寄送給使用者。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，例如電子郵件或手機號碼，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令牌（Token），一般是亂數產生的英數字，使用者接收後須於時效內進行輸入回傳動作，系統檢查回傳令牌有效性後，允許使用者重設密碼。
27	5. 授權與存取控制	5.1 執行功能及存取資源前，檢查使用者授權	說明：系統中除了公開區域外，任何執行功能及存取資源動作前，應檢查使用者已通過身分驗證且使用者具備權限可執行該功能或存取該項資源。
28		5.2 採用伺服端的集中過濾機制檢查使用者授權	說明：檢查使用者是否具備存取功能或資源之機制，應位於伺服器端且採用全面性集中控管機制(例如採用網站過濾器 Filter 機制)，明確設定檢查範圍。檢查機制位於伺服器端可以避免被攻擊者繞過檢查的問題，全面性集中控管可以避免人為疏漏導致可能有功能未檢查使用者授權之問題。

項次	分類	檢查項目	說明
29		5.3 對使用者/角色，僅賦予所需要的最低權限	說明：明確定義系統中角色及對應的權限，系統上線驗收時，應審查使用者賦予的角色及其取得的權限是否適當，系統上線後亦定期審查使用者所擁有的角色與權限清單。相關資訊宜提供系統介面以供查詢或匯出。
30		5.4 軟體程序（process）及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限執行	說明：系統之軟體程序或伺服器服務，若以系統最高權限或管理員權限啟動，將造成攻擊者成功入侵伺服器時，可以取得作業系統最高權限。應於作業系統增加服務專用之使用者，並授予執行伺服器服務及讀寫相關檔案的有限範圍權限，使其可以正常執行軟體程序作業，同時避免過高權限之風險。
31		5.5 除特殊管理者權限外，其他角色或權限無法修改系統中授權資料及存取控制列表（ACL）	說明：存取控制列表是用來表示系統使用者具有哪些權限的清單，實際上可能由多張表格組成，包含使用者清單、角色清單、權限清單、角色與權限關聯清單及使用者與角色關聯清單等。系統應確保只有特定管理員權限可以透過介面或具備資料庫權限可以修改存取控制列表，一般使用者無存取控制列表之修改權限。
32		5.6 重要行為由多人/角色授權後才得以進行	說明：設計軟體功能時將條件設定在兩個或多個以上，且需要滿足所有的條件才能完成作業時，稱之為職責分離（SeparationofDuties）。系統重要行為可以採取須通過多人/角色授權後才得以進行之設計。職責分離可以減少單一人員或資源由於權限過大，所可能造成的安全危害。實行職責分離再加上行為的稽核紀錄，可以防範內部舞弊的情況發生。
33		5.7 具有防範「跨站請求偽造」（Cross-SiteRequestForgery，CSRF）攻擊之措施	說明：「跨站請求偽造」攻擊發生情況為，攻擊者知道網站特定行為的執行參數，在使用者已通過網站身分驗證登入後，以欺騙使用者點選連結或其他方式，偽造使用者之請求進行該特定行為並帶入相關參數，以遂行惡意之目的。防範 CSRF 的措

項次	分類	檢查項目	說明
			施主要有：1.重要行為前先動態產生獨立而唯一的 requesttoken，並於執行行為前檢查。2.要求使用者重新身分驗證或證明該動作是人為進行（使用 CAPTCHA）。此安全需求項目僅適用於 WEB 網站系統。
34	6.日誌紀錄	6.1 針對身分驗證失敗、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進行日誌紀錄	說明：系統留存日誌紀錄之目的包含程式除錯、行為歸責、稽核取證及法規要求等。紀錄身分驗證失敗、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，將有助於定期稽核系統行為及資安事件追查。
35		6.2 日誌紀錄包含以下項目： 1.識別使用者之 ID（不可為個資類型）。 2.經系統校時後的時間戳記。 3.執行的功能或存取的資源。 4.事件類型或等級（priority）。 5.事件描述	說明：日誌紀錄宜考慮包含： 1.使用者 ID，不可為個資類型，避免共用帳號之情。 2.時間，系統應設定定期校時，應紀錄至微秒等級。 3.執行之功能或存取之資源名稱。 4.事件類型或優先等級。 5.執行結果或事件描述。 6.事件發生當下相關物件資訊。 7.網路來源與目的位址。 8.錯誤代碼，便於事件追查。
36		6.3 採用單一的日誌紀錄機制，確保輸出格式的一致性	說明：系統日誌紀錄應盡可能採用單一的 Log 機制，例如同一伺服器軟體應產出相同格式之日誌紀錄，以便於事件比對與追查。
37		6.4 對日誌紀錄進行適當保護及備份，避免未經授權存取	說明：系統產生日誌紀錄後，應定時將日誌紀錄進行遠端備份，並將檔案設定存取權限限制，避免未經授權存取。
38	7. 會談（Session）管理	7.1 使用者的會談階段，設定該帳號在合理的時間（至多 30 分鐘）內未活動即自動失效	說明：會談（Session）機制目的為管理使用者與伺服器之間的連線狀態，通常於客戶端首次連線伺服器即建立一會談識別碼（SessionID），並將使用者後續於系統中的相關資訊與該會談識別碼關連，以維持使用者相關資訊狀態。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，以避免

項次	分類	檢查項目	說明
			資安風險。
39		7.2 使用者的會談階段在登出後失效	說明：系統應有手動機制，使用者明確進行登出後，將該使用者的會談階段設為失效。
40		7.3 會談識別碼(SessionID)或使用者 ID 避免顯示於使用者可以改寫處（例如網址列）	說明：會談識別碼（SessionID）顯示於使用者可以改寫處，則有遭到暴力破解或嘗試猜測合法會談識別碼之可能性，應予避免。
41		7.4 會談識別碼(SessionID)採亂數隨機產生且不可預測	說明：為避免會談識別碼（SessionID）被猜測，建議儘量使用各種開發架構(J2EE、ASP.NET、PHP）所提供的內建 SessionID 產生管理方式，而不要自己產生 SessionID，以確保 SessionID 具隨機性與夠強健而不易被推測。
42		7.5 使用者登入後，重新賦予會談識別碼（SessionID）	說明：針對會談識別碼（SessionID）的 SessionFixation 攻擊，攻擊者在目標使用者登入前置換掉其所使用的 SessionID，使用者登入後將取得系統權限，攻擊者利用其已知的這組 SessionID 便可以偽冒成目標。伺服器在使用者初次連結網頁時（通常為首頁）給予 SessionID，登入後若仍採用相同 SessionID 則具有此風險。
43	8. 錯誤及例外管理	8.1 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息	說明：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。
44		8.2 所有功能皆進行錯誤及例外處理，並確保將資源正確釋放	說明：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。

項次	分類	檢查項目	說明
45		8.3 具備系統嚴重錯誤之通知機制（例如電子郵件或簡訊）	說明：系統增加電子郵件或簡訊之通知機制，並就系統錯誤或例外狀況進行等級區分，當嚴重等級錯誤發生時，採用通知機制，使系統管理員或相關人員得以即時得知錯誤發生，進行後續處理。
46	9.組態管理	9.1 管理者介面限制存取來源或不允許遠端存取	說明：管理者介面通常可執行系統中較高權限的功能(例如權限與人員管理)，其相對風險較高，因此應盡可能不允許遠端存取，僅允許透過內部網路存取，以避免有心人士從外部嘗試攻擊之可能。若有必要允許外部遠端存取管理者介面，應限制特定存取來源 IP，避免全面性開放存取。
47		9.2 作業平台定期更新並關閉不必要服務及埠口（Port）	說明：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，盡可能關閉不必要之項目，並正面表列需要開啟該服務及埠口（Port）之理由。
48		9.3 系統依賴的外部元件或軟體，不使用預設密碼	說明：表列系統所使用的外部元件與軟體，包含其版本資訊，並檢核確認未有使用預設密碼之情況。
49		9.4 參數設定或系統設定存放處，限制存取或進行適當保護	說明：系統參數設定檔案，應設置適當檔案權限，避免被非授權存取。
50		9.5 針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新	說明：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。注意相關之安全漏洞通告(透過 CVEDetails 網站、廠商安全通告等)，於系統驗收前確認採用之軟體與元件，已使用最新之穩定版本或該版本已排除所有已知安全漏洞。系統上線後，持續定期關注安全漏洞通告，若有相關之安全漏洞發生，評估該系統元件更新之必要性，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。

內政部委外服務案個人資料保護規範

一、 機關委託廠商蒐集、處理或利用個人資料及檔案時，應遵守本規範相關規定。

二、 蒐集、處理或利用時之義務

（三） 廠商依契約規定蒐集、處理或利用個人資料時，應遵守個人資料保護法、該法施行細則及內政部（以下簡稱本部）個人資料保護管理制度等相關規定。

（四） 廠商不得利用機關提供或履行契約蒐集之個人資料及檔案，為自己或他人利益從事契約履約目的範圍以外之處理或利用行為，或以任何方式或方法交付予履約無關之第三人。

（五） 廠商僅得於機關以下指示之範圍內，蒐集、處理或利用個人資料：

■預定蒐集、處理、利用

範圍：新一代國民身分證換發系統建置及維護案

蒐集資料：處理戶役政業務及自然人憑證業務所蒐集之相關個資

期間：本案履約期間

□其他：

三、 安全（維護）措施

廠商在履行契約所必須之範圍內，應依個人資料保護法第二十七條第一項規定採行個人資料保護法施行細則第十二條所規定適當之安全（維護）措施。

四、 複委託之約定如下：

□機關及廠商約定複委託予第三人執行時，廠商負有下列義務：

(一) 廠商履行契約前，就涉及蒐集、處理或利用個人資料或檔案之業務擬複委託予第三人執行者，應提出受複委託第三人之名稱、地址、符合第二點第三款之執行業務範圍、

對該第三人設置之監督機制及保密同意書等文件，經機關審查通過，並以書面同意後始得辦理。

(二) 廠商應依第二點規定限定受複委託第三人蒐集、處理、利用個人資料之範圍，並對該受複委託第三人依個人資料保護法及本部個資保護管理制度等相關規定進行適當之監督。

(三) 受複委託第三人於委託範圍內蒐集、處理、利用個人資料之行為，視同廠商行為，廠商應負所有責任。

□廠商執行契約，就涉及蒐集、處理或利用個人資料或檔案之業務，不得複委託第三人執行。

五、 當事人權利行使時之義務

機關受理當事人依個人資料保護法第三條規定行使當事人權利時，廠商應於機關指定期限內，配合提供資料或提出說明；當事人如逕向廠商或受其複委託第三人行使個人資料保護法第三條所定權利者，廠商或受其複委託第三人除應依相關規定辦理，並應於三十日內將處理情形以書面通知機關備查。

六、 配合義務

（一） 廠商依個人資料保護法第十五條第二款或第十六條但書第七款規定，經當事人同意而為蒐集、處理或特定目的外利用前，應將該同意內容與取得方式送交機關審查。廠商依個人資料保護法第六條第一項第六款規定，經當事人書面同意而為蒐集、處理及利用者，亦同。

（二） 機關於契約期間內，得要求廠商提供或說明涉及個人資料業務之處理事項，並提供相關資料，廠商不得拒絕。

（三） 必要時，機關得要求廠商於簽約後一個月內參考機關個人資料保護相關規範，訂定「個人資料保護專案計畫書」送機關備查，計畫書中應包含個人資料保護法令及機關要求之安全維護事項。若有變更計畫內容，應函送機關備查。

七、 個人資料事故通知義務

廠商因履行契約，致個人資料被竊取、洩漏、竄改或其他侵害之情形時，於發現後，應立即通知本部，並採取因應措施；廠商於查明後應將其違反情形、涉及個人資料範圍、採行及預定採行之補救措施通知本部，經本部同意後，依法以適當方式通知當事人。

八、 定期確認

（一） 機關得針對廠商個人資料安全管理措施實施情形進行審查，並將審查結果作成紀錄備查；必要時，得派員進行實地訪查或委託專業人員進行查核，廠商應予配合。

（二） 機關於訪查或查核後，認有缺失，得以書面敘明理由通知廠商限期改善。

九、 損害賠償責任

（一） 廠商違反本規範第二點至第七點、第八點第一款、第十點或經機關依第八點第二款限期改善而屆期未改善，機關得依契約規定處理；若機關受有損害，並得請求損害賠償。

（二） 廠商因履行契約而有違反個人資料保護法、個人資料保護法施行細則等規定，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。

（三） 機關因廠商履行契約違反個人資料保護法或其施行細則而受有損害時，得向廠商請求損害賠償。若因此遭第三人請求損害賠償時，應由廠商負責處理並承擔一切法律責任；如於訴訟中，廠商應協助機關為必要之答辯及提供相關資料，並應負擔因此所生之訴訟費用、律師費用及其他相關費用，並負責清償機關對第三人所負之損害賠償責任。

十、 履約中或契約終止時資料之刪除或返還

（一） 除機關、廠商雙方另有約定或法律另有規定外，廠商應於履約期限屆滿或經機關要求時，將因履行契約而取得之個人資料及檔案全數返還予機關，其備份應全數銷毀刪除，不得以任何形式自行留存、保留存取權限或提供予第三人利用；並提供刪除、銷毀或返還個人資料之時間、方式、地點等紀錄備查。

（二） 前款返還，廠商得向機關指定之第三人交付之。

（三） 第一款刪除、銷毀作業，廠商應於作業前一日通知機關，機關得於必要時派員進行實地查訪或委託專業人員進行查核，廠商應予配合。