資通系統資安需求項目查檢表

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
存取控制	3.2.1.1.1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，因此應具備帳號管理機制，可對系統帳號進行申請、建立、修改、啟用、停用或刪除之行為。	V	V	V	
	3.2.1.1.2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。		V	V	
	3.2.1.1.3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。		V	V	
	3.2.1.1.4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。			V	
	3.2.1.1.5應依機關規定	應依據機關規定之情況			V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
	之情況及條件，使用資通系統。	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)。				
	3.2.1.1.6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)。			V	
	3.2.1.1.7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。	V	V	V	
	3.2.1.1.8遠端存取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。	V	V	V	
	3.2.1.1.9遠端存取應採用加密機制。	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。	V	V	V	
事件日	3.2.1.2.1訂定日誌之記錄時間週期及留存政策，並保留日誌至少6	應依機關規定之時間週期及紀錄留存政策，保留系統事件日誌(Audit	V	V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
誌與可歸責性	個月。	Logs)，目的包含程式除錯、行為歸責、稽核取證及法規要求等。				
	3.2.1.2.2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。	資通系統應實作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。	V	V	V	
	3.2.1.2.3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，有助於定期記錄系統行為及資安事件追查。	V	V	V	
	3.2.1.2.4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，採用單一日誌機制，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。	日誌應詳細描述所觸發的事件，包含人、事、時、地、物等關鍵資訊，宜包含：使用者帳號(避免個資類型)、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。系統開發人員應盡可能採用單一的Log機制，如不得同時混用兩種以上日誌產生套件(如	V	V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
		Log4Net與Nlog等)，並應確保日誌內容格式之可讀性，以便於事件比對與追查。日誌應依據資通安全政策及其他法規要求，納入任何有必要留存之資訊，如憑證資訊、日誌層級、會談識別碼等。				
	3.2.1.2.5資通系統於日誌處理失效時，應採取適當之行動。	當資通系統發生日誌處理失效狀況時，應採取相對應的處理措施(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缺乏系統日誌以供比對追查之情況。	V	V	V	
	3.2.1.2.6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處理失效事件、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。			V	
	3.2.1.2.7資通系統應使用系統內部時鐘產生日	使用系統內部時鐘產生日誌所需時戳，如	V	V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
	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)。	Windows作業系統顯示之日期時間等。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。				
	3.2.1.2.8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定期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。		V	V	
	3.2.1.2.9對日誌之存取管理，僅限於有權限之使用者。	應施行日誌存取控管，避免未經授權使用者惡意讀取、竄改或刪除日誌紀錄。	V	V	V	
	3.2.1.2.10應運用雜湊或其他適當方式之完整性確保機制。	應保護系統日誌之完成性，避免未經授權的竄改行為。如使用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。其他保護方式如加密、唯讀保存		V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
		及即時監視檔案異動行為等。				
	3.2.1.2.11定期備份日誌至與原系統外之其他實體系統。	定期進行日誌異機備份，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備份，可降低因系統損毀或人為惡意刪除之風險。			V	
識別與鑑別	3.2.1.3.1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使用者之功能，如為內部使用者建立個別帳號，以強化系統之可歸責性。多人共用帳號行為會造成難以藉由日誌識別使用者身分。	V	V	V	
	3.2.1.3.2內部使用者對資通系統之存取採取多重認證技術。	多重認證技術係指MFA，意即身分驗證時應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)。使用情境範例如系統管理者透過自然人憑證登入系統後台服務，同時具備所知之事(PIN碼)與所持之物(憑證卡片)之要求。			V	
	3.2.1.3.3使用預設密碼	使用者註冊時係由資通	V	V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
	登入系統時，應於登入後要求立即變更。	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。				
	3.2.1.3.4身分驗證相關資訊不以明文傳輸。	身分驗證相關資訊於網路傳輸時，不可直接傳輸明文(如密碼原始字串)，避免被惡意攔截網路封包而外洩。	V	V	V	
	3.2.1.3.5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，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。	V	V	V	
	3.2.1.3.6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。	應強制最低密碼複雜度，包含密碼長度限制及組成字元種類，避免密碼被輕易破解。密碼最短效期可防止使用者為規避密碼歷程限制而於短期內頻繁變換密碼後又改回原始密碼。強制最長之效期之目的在避免固定使用同一組密碼。實務上，可參考政府組態基準(Government Configuration Baseline, GCB)[1]之建議值，設定密碼複雜度及密碼使用效期限制。	V	V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
	3.2.1.3.7 密碼變更時，至少不可以與前3次使用過之密碼相同。	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。	V	V	V	
	3.2.1.3.8 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。		V	V	
	3.2.1.3.9 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		V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
		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。				
	3.2.1.3.10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。	V	V	V	
	3.2.1.3.11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		V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
		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。				
	3.2.1.3.12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。	V	V	V	
系統與服務獲得	3.2.1.4.1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	V	V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
		正確釋放。				
	3.2.1.4.2具備系統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。			V	
	3.2.1.4.3資通系統相關軟體，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。	V	V	V	
系統與通訊保護	3.2.1.5.1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。			V	
	3.2.1.5.2使用公開、國際機構驗證且未遭破解	若使用自行創造的加密方式且未經過適當的驗證程			V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
	之演算法。	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-256以上之雜湊演算法等。				
	3.2.1.5.3支援演算法最大長度金鑰。	當設定HTTPS傳輸加密演算法(Cipher)時，應盡量使用作業系統與伺服器所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。			V	
	3.2.1.5.4資通系統重要組態設定及其他具保護需求之資訊應加密或以其他適當方式儲存。	保護資訊的機密性為資通安全之重點，包含資通系統重要組態設定(如資料庫連線資訊等)以及任何具保護需求之資訊皆應實作機密保護機制避免外洩。			V	
系統與資訊完整性	3.2.1.6.1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		V	V	

技術面資安需求						
分類	安全需求項目	說明	適用分級			評量結果(是/否/不適用)
			普	中	高	
		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。				
	3.2.1.6.2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。		V	V	

管理面安全需求					
安全需求項目	說明	適用分級			評量結果(是/否/不適用)
		普	中	高	
3.2.2.1.1依據日誌儲存需求，配置所需之儲存容量。	資通系統應配置日誌所需之儲存容量(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。	V	V	V	
3.2.2.2.1針對系統安全需求(含機密性、可用性、完整性)，進行確認。	建議可使用本附件進行系統安全需求檢核。	V	V	V	
3.2.2.2.2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。	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		V	V	

管理面安全需求					
安全需求項目	說明	適用分級			評量結果(是/否/不適用)
		普	中	高	
	動，包含「安全設計原則」，進行系統設計時應參考使用的設計原則；「執行攻擊面分析」，進行攻擊面的定義、識別與對應方式，包含如何進行攻擊面的衡量與評估，並進行管理等；「執行風險分析」，軟體設計過程中，如何透過使用威脅建模與架構風險分析，進行系統架構與威脅的分析，並使用通用性的安全設計原則與控制措施，提供軟體安全風險分析與控制；「安全設計審查」，在進行一連安全軟體設計的實務活動之後，應確保安全設計符合需求階段提出的相關安全需求及安全設計，以符合軟體安全的基準線。				
3.2.2.2.3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。		V	V	
3.2.2.2.4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	V	V	V	

管理面安全需求					
安全需求項目	說明	適用分級			評量結果(是/否/不適用)
		普	中	高	
	制措施，輔以檢核表方式進行確認，可減少遺漏之可能。				
3.2.2.2.5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 TOP10[4]或CWE/SANS TOP25[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。	V	V	V	
3.2.2.2.6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。實務上，常使用自動化檢測工具以提高檢測效率，輔以有經驗之軟體開發人員進行檢測結果檢視及分析，檢測工具可參考OWASP組織整理之免費及商業化工具列表[6]。			V	
3.2.2.2.7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。	V	V	V	
3.2.2.2.8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			V	

管理面安全需求					
安全需求項目	說明	適用分級			評量結果(是/否/不適用)
		普	中	高	
	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。				
3.2.2.2.9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。	V	V	V	
3.2.2.3.1加密金鑰或憑證週期性更換。	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。			V	
3.2.2.4.1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。	V	V	V	

管理面安全需求					
安全需求項目	說明	適用分級			評量結果(是/否/不適用)
		普	中	高	
3.2.2.4.2應定期執行軟體與資訊完整性檢查。	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。			V	

1. 參考文獻

[1] 行政院國家資通安全會報技術服務中心。政府組態基準(GCB)。https://www.nccst.nat.gov.tw/GCB
[2] OWASPSecureHeadersProject。https://www.owasp.org/index.php/OWASP_Secure_Headers_Project
[3] 行政院國家資通安全會報技術服務中心(103年1月)。「安全軟體設計參考指引」。
[4] OWASP,OWASPTopTenProject。https://owasp.org/
[5] SANS,CWE/SANSTOP25MostDangerousSoftwareErrors。https://cwe.mitre.org/index.html
[6] OWASP,SourceCodeAnalysisTools。https://owasp.org/