國藝會財務資訊系統建置案
應用系統安全需求項目說明

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
機密性	1.1 機敏資料傳輸時，採用加密機制	V	V	V	通用
	1.2 使用公開、國際機構驗證且未遭破解的演算法			V	通用
	1.3 使用演算法支援的最大長度金鑰			V	通用
	1.4 加密金鑰或憑證週期性更換		V	V	通用
	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			V	通用
	1.6 機敏資料儲存時，採用加密機制			V	通用
完整性	2.1 於伺服器端以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性	V	V	V	通用
	2.2 針對開放下載的資料，也提供資料之雜湊值(HASH Value)供使用者比對其完整性		V	V	通用
	2.3 具有防範 SQL 命令注入攻擊(SQL Injection)之措施	V	V	V	通用
	2.4 具有防範跨站腳本攻擊(Cross-Site Scripting)之措施	V	V	V	WEB
	2.5 驗證網頁重導(Redirects)與導向(Forwards)之目的地在合法名單內		V	V	WEB
	2.6 重要系統資料或紀錄留存雜湊值以確保完整性			V	通用
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	V	V	V	通用
	3.2 採用「高可用性」(High Availability) 架構(分散式或叢集伺服器架構)			V	通用
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	V	V	V	通用

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
	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)		V	V	通用
	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		V	V	通用
	4.4 確實規範使用者密碼強度 (密碼長度 8 個字元以上、包含英文大小寫、數字，以及特殊字元)		V	V	通用
	4.5 使用者必須定期更換密碼，且至少不可以與前 3 次使用過之密碼相同	V	V	V	通用
	4.6 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及來源 IP 繼續嘗試登入	V	V	V	通用
	4.7 身分驗證相關資訊不以明文傳輸	V	V	V	通用
	4.8 密碼添加亂數(Salt)進行雜湊函式(HASH Function)處理後，分別儲存亂數及雜湊後密碼			V	通用
	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		V	V	通用
	4.10 重要交易行為要求使用者再次進行身分驗證			V	通用
	4.11 採用多重因素身分驗證(兩種以上驗證類型)			V	通用
	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		V	V	通用
授權與存取	5.1 執行功能及存取資源前，檢查使用者授權	V	V	V	通用
	5.2 採用伺服端的集中過濾機制檢查使用者授權		V	V	通用
	5.3 對使用者/角色，僅賦予所需要的最低權限		V	V	通用

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
	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			V	通用
	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)			V	通用
	5.6 重要行為由多人/角色授權後才得以進行			V	通用
	5.7 具有防範「跨站請求偽造」(Cross-Site Request Forgery，CSRF)攻擊之措施	V	V	V	WEB
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記錄	V	V	V	通用
	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	V	V	V	通用
	6.3 採用單一的日誌紀錄機制，確保輸出格式的一致性	V	V	V	通用
	6.4 對日誌紀錄進行適當保護及備份，避免未經授權存取	V	V	V	通用
會談	7.1 使用者的會談階段，設定該帳號在合理的時間(至多 60 分鐘)內未活動即自動失效	V	V	V	通用
	7.2 使用者的會談階段在登出後失效	V	V	V	通用
	7.3 會談識別碼(Session ID)或使用者 ID 避免顯示於使用者可以改寫處(例如網址列)		V	V	通用
	7.4 會談識別碼(Session ID)採亂數隨機產生且不可預測			V	通用
	7.5 使用者登入後，重新賦予會談識別碼(Session ID)			V	通用

安全特性分類	安全需求項目	適用分級			適用類型
		普	中	高	
錯誤及例外	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	V	V	V	通用
	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		V	V	通用
	8.3 具備系統嚴重錯誤之通知機制(例如電子郵件或簡訊)			V	通用
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	V	V	V	通用
	9.2 作業平台定期更新並關閉不必要服務及埠口(Port)		V	V	通用
	9.3 系統依賴的外部元件或軟體，不使用預設密碼		V	V	通用
	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			V	通用
	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			V	通用