文化內容策進院
系統安全需求檢核表

填寫日期：　　年　　月　　日

分類	問題	答案 (是/否/不適用)	說明
機密性	機敏資料傳輸時，採用加密機制		
	機敏資料儲存時，採用加密機制		
	使用公開、國際機構驗證且未遭破解的演算法		
	使用該演算法支援的最大金鑰長度		
	不使用自行創造的加密方式		
	加密金鑰具有保護機制		
	加密金鑰或憑證週期性更換		
完整性	重要資料產生雜湊(HASH)值，確保其完整性		
	重要資料傳輸過程，使用防止竄改的協定		
	提供下載的資料，產生雜湊(HASH)值供比對其完整性		
可用性	評估服務重要性，設定可用性要求		
	採用「高可用性」(High Availability) 架構或機制		
	重要資料定時同步至備援環境		
輸入驗證	採用過濾機制，以防止輸入惡意命令或資料		
	驗證使用者輸入資料		
	驗證外部取得的資料		
	驗證系統參數合理性		
	於伺服器端檢查輸入資料合法性		
身分認證	除了允許匿名存取的功能外，所有功能都必須經過認證才允許存取		
	身分認證機制位於伺服端且採用集中管理機制		
	採用多重因素認證(兩種以上認證類型)		
	採用驗證碼(CAPTCHA)機制於身分認證或重要交易行為，以防範自動化程式之嘗試		
	身分認證相關資訊不以明文傳輸		
	身分認證相關資訊不存於源碼中，並限制存取		
	身分認證失敗達一定次數後鎖定該帳號		
	身分認證發生錯誤時，預設不允許存取任何非公開功能		
	密碼添加亂數資料(Salt)後進行雜湊函數(HASH)處理，才加以儲存		
	密碼須符合複雜度(長度限制、具備英文大小寫及特殊字元等)		
	限制需定期更換密碼		
	重要交易行為要求再次身分認證		
授權與存取控	採用伺服端的集中管理機制檢查使用者授權		
	執行功能或存取資源前，檢查使用者授權		

分類	問題	答案 (是/否/不適用)	說明
制	除特殊管理者權限外，其他角色或權限無法修改授權資料及存取控制列表(ACL)		
	使用者/角色賦予所需的最小權限		
	軟體程序(process)以最小的權限執行，不以系統管理員或最高權限執行		
	重要行為由多人/角色授權後才得以進行		
日誌紀錄	認證失敗、存取失敗、輸入驗證失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行Log記錄		
	Log紀錄考慮包含以下項目 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(例如，成功或失敗)。 5.事件優先權(priority)。 6.事件詳細描述。 7.事件代碼。 8.網路位址		
	採用單一的Log機制，確保輸出格式的一致性		
	Log進行適當保護及備份，避免未經授權存取		
會話管理	會話識別碼(Session ID)是隨機產生且不可預測		
	使用者的會話階段，設定在合理的時間內失效		
	使用者的會話階段，使用者登出後失效		
	使用者重新登入後，會話識別碼(Session ID)會改變		
	不將會話識別碼(Session ID)或使用者ID顯示於使用者可以改寫處		
錯誤及例外管理	所有的功能都會進行錯誤及例外處理，並將資源正確釋放		
	軟體發生錯誤時，使用者頁面僅顯示簡短的錯誤訊息及代碼，不包含詳細的錯誤訊息或除錯用訊息		
	嚴重錯誤採用通知機制(例如電子郵件或簡訊)		