國立臺灣藝術大學			
機密等級：□普通 □敏感 □密	修訂日期： 2024/06/07		版本 V1.1
資通系統防護基準檢核表(普)		表單編號：03-010-05-□□□□-□□□ (表單編號：XXXX-XXX西元年後兩碼加上兩碼月份-三碼流水號)	
資通系統網站名稱：			
資通系統網站網址 / IP：			
檢核項目	**適用分級**	**檢查結果**	**說明或佐證**
構面: 存取控制			
措施: 帳號管理			
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。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施: 遠端存取			
1.對於每一種允許之遠端存取類型(如遠端桌面連線、ssh、網路芳鄰或FTP)，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。	普|中|高	□符合 □部分符合 □不符合 □不適用	
2.使用者之權限檢查作業應於伺服器端完成。	普|中|高	□符合 □部分符合 □不符合 □不適用	
3.應監控資通系統遠端連線。	普|中|高	□符合 □部分符合 □不符合 □不適用	
4.資通系統應採用加密機制。	普|中|高	□符合 □部分符合 □不符合 □不適用	
構面: 事件日誌與可歸責性			
措施: 記錄事件			
1.訂定日誌之記錄時間週期及紀錄留存政策，並保留日誌至少六個月。	普|中|高	□符合 □部分符合 □不符合 □不適用	
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。	普|中|高	□符合 □部分符合 □不符合 □不適用	
3.應記錄資通系統管理者帳號所執行之各項功能。	普|中|高	□符合 □部分符合 □不符合 □不適用	

檢核項目	適用分級	檢查結果	說明或佐證
措施:日誌紀錄內容			
1.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。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:日誌儲存容量			
1.依據日誌紀錄(Audit Logs)儲存需求，配置所需之儲存容量。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:日誌處理失效之回應			
1.資通系統於日誌處理失效時，應採取適當之行動。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:時戳及校時			
1.資通系統應使用系統內部時鐘產生日誌紀錄(Audit Logs)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)。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:日誌資訊之保護			
1.對日誌(Audit Logs)之存取管理，僅限於有權限之使用者。	普|中|高	□符合 □部分符合 □不符合 □不適用	
構面: 營運持續計畫			
措施: 系統備份			
1.訂定系統可容忍資料損失之時間要求。	普|中|高	□符合 □部分符合 □不符合 □不適用	
2.執行系統源碼與資料備份。	普|中|高	□符合 □部分符合 □不符合 □不適用	
構面: 識別與鑑別			
措施: 內部使用者之識別與鑑別			
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。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:身分驗證管理			
1.使用預設密碼登入系統時，應於登入後要求立即變更。	普|中|高	□符合 □部分符合 □不符合 □不適用	

檢核項目	適用分級	檢查結果	說明或佐證
2.身分驗證相關資訊不以明文傳輸。	普|中|高	□符合 □部分符合 □不符合 □不適用	
3.具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次，至少15分鐘內不允許該帳號繼續嘗試或使用機關自建之失敗驗證機制。	普|中|高	□符合 □部分符合 □不符合 □不適用	
4.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。(但對於非內部使用者可依機關自行規範辦理)	普|中|高	□符合 □部分符合 □不符合 □不適用	
5.密碼變更時，至少不可以與前三次使用過之密碼相同。(但對於非內部使用者可依機關自行規範辦理)	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施: 鑑別資訊回饋			
1.資通系統應遮蔽鑑別過程中之資訊。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施: 非內部使用者之識別與鑑別			
1.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)。	普|中|高	□符合 □部分符合 □不符合 □不適用	
構面: 系統與服務獲得			
措施: 系統發展生命週期需求階段			
1.針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:系統發展生命週期開發階段			
1.應針對安全需求實作必要控制措施。	普|中|高	□符合 □部分符合 □不符合 □不適用	
2.應注意避免軟體常見漏洞及實作必要控制措施。	普|中|高	□符合 □部分符合 □不符合 □不適用	

檢核項目	適用分級	檢查結果	說明或佐證
3.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。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:系統發展生命週期測試階段			
1.執行「弱點掃描」安全檢測。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:系統發展生命週期部署與維運階段			
1.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。	普|中|高	□符合 □部分符合 □不符合 □不適用	
2.資通系統相關軟體，不使用預設密碼。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:系統發展生命週期委外階段			
1.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。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施: 系統文件			
1.應儲存與管理系統發展生命週期之相關文件。	普|中|高	□符合 □部分符合 □不符合 □不適用	
構面: 系統與資訊完整性			
措施: 漏洞修復			
1.系統之漏洞修復應測試有效性及潛在影響，並定期更新。	普|中|高	□符合 □部分符合 □不符合 □不適用	
措施:資通系統監控			
1.發現資通系統有被入侵跡象時，應通報機關特定人員。	普|中|高	□符合 □部分符合 □不符合 □不適用	

維護廠商- 填表人員(簽名) ：

維護廠商- 單位主管(簽核) ：