國立清華大學計算機與通訊中心

主機資訊安全自我檢核表

紀錄編號：

版本：20090619

主機名稱		檢核人員		檢核日期	年　月　日

S1.主機安全檢核				
1.作業系統安全	必要	檢核內容	檢核結果	備　註
	*	1.是否具備版本更新機制？	□是 □否	□手動 □自動
		2.是否隱藏作業系統版本資訊？	□是 □否	
		3.是否安裝防毒軟體？	□是 □否	
		4.是否定期更新防毒軟體病毒碼？	□是 □否	□手動 □自動
	*	5.是否安裝防火牆系統？	□是 □否	
		6.是否安裝主機型入侵偵測/防禦系統？	□是 □否	
		7.是否定期更新入侵偵測/防禦系統之特徵資料庫？	□是 □否	□手動 □自動
		8.是否安裝惡意程式偵測系統？	□是 □否	
	*	9.是否針對使用需求開放不同之目錄存取權限？	□是 □否	
	*	10. 是否檢查開放存取之目錄有無存在異常程式？	□是 □否	
		11. 是否定期審閱系統紀錄檔案？	□是 □否	
		12. 是否要求定期更換系統管理密碼？ 多久一次？	□是 □否	更換週期 _____
	*	13. 系統管理密碼的長度是否最少 8 碼？	□是 □否	
	*	14. 系統管理密碼是否避免使用易猜或公開資訊？	□是 □否	
		15. 是否定期備份作業系統及紀錄檔案？	□是 □否	
		16. 是否定期進行弱點掃瞄或驗證？	□是 □否	
2.應用服務安全	必要	檢核內容	檢核結果	備　註
	*	1.是否具備版本更新機制？	□是 □否	□手動 □自動
		2.是否隱藏應用服務版本資訊？	□是 □否	
	*	3.是否僅開放系統對外所需之相關應用服務？	□是 □否	
	*	4.是否移除系統不必要之應用服務？	□是 □否	
		5.是否審閱應用服務開放或執行的狀態？	□是 □否	

	*	6. 是否啟動應用服務紀錄機制（如:IIS、Apache…）？	□是 □否	
		7. 是否定期審閱應用服務系統紀錄檔案？	□是 □否	
S2.網路連線設定安全檢核				
1. 遠端系統管理	必要	檢核內容	檢核結果	備　註
	*	1. 是否僅開放特定網路地址進行遠端系統管理？	□是 □否	
		2. 是否採用安全的連線方式（如：SSH、VPN…）進行遠端系統管理？	□是 □否	
2. 網路連線控管	必要	檢核內容	檢核結果	備　註
	*	1. 是否針對不同應用服務開放原則設定相關網路連線存取政策？	□是 □否	
		2. 是否設定錯誤連線存取限制(如：錯誤 3 次即終止連線)？	□是 □否	
		3. 是否定期審閱網路連線紀錄？	□是 □否	
S3.應用軟體安全檢核				
1. 存取控制	必要	檢核內容	檢核結果	備　註
	*	1. 是否確保透過存取控制參數不能取得額外之服務權限？	□是 □否	
		2. 是否確保需要授權之系統資源經過充分的授權檢查才提供給用戶端使用？	□是 □否	
		3. 是否可透過修改 Session ID 取得其他使用者之帳號身份？	□是 □否	
	*	4. 是否有可能跳過登入檢查存取需要授權之頁面或功能？	□是 □否	
2. 使用者認證	必要	檢核內容	檢核結果	備　註
		1. 是否確保使用者只有在 SSL 保護下之頁面被要求送出憑證？	□是 □否	
	*	2. 是否確保認證程序無法被跳過？	□是 □否	
		3. 是否確保使用者名稱及密碼透過加密通道傳輸？	□是 □否	
	*	4. 是否移除預設帳號及密碼？	□是 □否	
		5. 是否要求使用者密碼之複雜度足夠讓密碼難以被猜測？	□是 □否	
		6. 是否提供錯誤密碼次數鎖定功能？	□是 □否	
	*	7. 是否要求使用者密碼不可空白？	□是 □否	

3. 目錄設定管理	必要	檢核內容	檢核結果	備　註
	*	1. 是否關閉目錄索引功能？	□是 □否	
		2. 是否僅開放部分應用系統所需之目錄讀取權限？	□是 □否	
	*	3. 是否僅開放應用軟體存取主機系統之特定目錄權限（如：應用軟體根目錄）？	□是 □否	
4. 應用程式設定管理	必要	檢核內容	檢核結果	備　註
		1. 是否關閉透過網際網路竄改系統資源之功能（如 HTML Method 之 PUT 及 DELETE）？	□是 □否	
	*	2. 是否已更新或修正應用程式存在之已知安全弱點？	□是 □否	
	*	3. 是否確保備份之原始碼檔案不可被公開存取？	□是 □否	
	*	4. 是否確保應用程式安裝後之預設檔案不會揭露機密資訊（如：J2EE 之 snoop.jsp 及 PHP 之 php_info()…）？	□是 □否	
	*	5. 是否備份設定資料？	□是 □否	
		6. 是否定期檢視應用程式設定資料是否被竄改？	□是 □否	
5. 錯誤訊息處理	必要	檢核內容	檢核結果	備　註
	*	1. 是否確保應用程式錯誤訊息不會顯示含有可供攻擊者利用之系統或程式資訊？	□是 □否	
	*	2. 是否確保應用程式自定之錯誤訊息不會提供任何可供攻擊者利用之資訊？	□是 □否	
6. 資料保護	必要	檢核內容	檢核結果	備　註
		1. 是否確保 HTML 中不含有敏感資料（如：帳號與密碼）？	□是 □否	
		2. 是否將儲存於資料庫之機敏性資訊（如：帳號與密碼）以編碼或加密方式處理？	□是 □否	
	*	3. 是否額外提供資料庫存取帳號，並依據功能限制其存取資料庫的權限？	□是 □否	
	*	4. 是否要求資料庫存取帳號之密碼複雜度足夠讓密碼難以被猜測？	□是 □否	
	*	5. 是否針對資料庫網路連線存取權限進行適當的限制？	□是 □否	
	*	6. 是否備份資料庫內容？	□是 □否	
	*	7. 是否將資料庫備份儲存於系統嚴格控管之目錄，而非保存	□是 □否	

		於應用軟體根目錄？		
7. 輸入值驗證	必要	檢核內容	檢核結果	備　註
	＊	1. 是否確保應用程式不允許輸入值包含腳本程式(Script)？	□是 □否	
	＊	2. 是否確保應用程式不會執行由客戶端輸入之 SQL 指令？	□是 □否	
	＊	3. 是否確保應用程式不會執行由客戶端輸入之作業系統指令？	□是 □否	
	＊	4. 是否針對輸入參數之特性設定適當之型別與長度？	□是 □否	
	＊	5. 是否針對輸入值進行特殊字元之過濾？	□是 □否	
8. 系統管理介面	必要	檢核內容	檢核結果	備　註
	＊	1. 是否確保基礎架構如網頁伺服器及應用程式伺服器之管理介面無法藉由網際網路存取，或僅允許特定網路地址存取？	□是 □否	
	＊	2. 是否確保應用程式之管理介面無法藉由網際網路存取，或僅允許特定網路地址存取？	□是 □否	

以下由維運單位填寫

審核結果

□通過（同意申請「安控服務」）

□未通過（不符合項目如下）

承 辦 人	日期_____	單位主管	日期_____

說明

1.「必要」欄位標示為＊者，表示該項檢核為必要通過檢核項目。
2.「必要」欄位標示為空白者，表示「建議」採用之安全措施。