

附件 5 核心資通系統安全防護評量表

表1 「核心資通系統評選表」編號 1 系統之防護評量表

1.系統環境資訊			
系統名稱		系統等級	<input type="checkbox"/> 高 <input type="checkbox"/> 中 <input type="checkbox"/> 普
系統性質	<input type="checkbox"/> 本地端程式 <input type="checkbox"/> 正式網站 <input type="checkbox"/> 測試網站 <input type="checkbox"/> 正式備援網站 <input type="checkbox"/> 其他：_____		
系統網址	<input type="checkbox"/> 無 <input type="checkbox"/> 有，前台網址為：_____ 後台網址為：_____ 其它網址為：_____		
系統主機服務與埠口 註：將依填寫內容檢測埠口開放狀態，請依現況填寫。	系統主機 IP	開放之埠口	目的原因
	(範例)127.0.0.1	80 443	HTTP HTTPS
	主機 1:		
	主機 2:		
	主機 3:		
多重因素認證	身分驗證是否提供多重因素認證： <input type="checkbox"/> 否 <input type="checkbox"/> 是，請說明登入方式： (範例：帳號密碼 + 簡訊驗證碼) _____ + _____		
連線核心資通系統進行檢測時，「用戶端」須具備條件(可多選)	<input type="checkbox"/> 無特定要求 <input type="checkbox"/> 有(僅支援下列項目，請勾選) 作業系統 <input type="checkbox"/> XP <input type="checkbox"/> Win 7 <input type="checkbox"/> Win 8.x <input type="checkbox"/> Win 10 以上 作業系統位元 <input type="checkbox"/> 32 位元 <input type="checkbox"/> 64 位元 瀏覽器 <input type="checkbox"/> IE8 <input type="checkbox"/> IE9 <input type="checkbox"/> IE10 <input type="checkbox"/> IE11 <input type="checkbox"/> Edge <input type="checkbox"/> Chrome <input type="checkbox"/> FireFox		

	<p>瀏覽器位元要求 <input type="checkbox"/>32 位元 <input type="checkbox"/>64 位元</p> <p><input type="checkbox"/>作業系統必須加入 AD 網域</p> <p>必須使用下列元件：</p> <p><input type="checkbox"/>.NET Framework，版本_____</p> <p><input type="checkbox"/>VC++ Runtime，版本_____</p> <p><input type="checkbox"/>JRE，版本 _____</p> <p><input type="checkbox"/>必須使用卡片和讀卡機登入</p> <p><input type="checkbox"/>必須使用自然人憑證登入</p> <p><input type="checkbox"/>其他，請說明：_____</p>
<p>2.系統防護評量</p>	
<p>類別</p>	<p>評量項目</p>
<p>普級以上系統適用項目</p>	
<p>識別與鑑別</p>	<ol style="list-style-type: none"> 1. 使用預設密碼登入系統時，應於登入後要求立即變更。 2. 身分驗證相關資訊不以明文傳輸。 3. 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。 <p style="background-color: yellow;">註：請說明登入失敗達_____次，鎖定_____分鐘。如前後台設置不一致請分別提供說明。</p> 4. 使用密碼進行驗證時，應強制最低密碼複雜度。 5. 密碼變更時，至少不可以與前 3 次使用過之密碼相同。 6. 資通系統應遮蔽鑑別過程中之資訊。
<p>系統與服務獲得</p>	<ol style="list-style-type: none"> 7. 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。 8. 執行「弱點掃描」安全檢測。 <p style="background-color: yellow;">註：請提供檢測報告及修補紀錄。</p>

	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。
中級以上系統適用項目	
存取控制	10. 採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。
識別與鑑別	11. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。
	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符記。
系統與資訊完整性	13. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。
高級系統適用項目	
存取控制	14. 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。 註：請提供允許閒置時間____分。如前後台設置不一致請分別提供說明。
識別與鑑別	15. 對資通系統之存取採取多重認證技術。
系統與通訊保護	16. 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。
	17. 使用公開、國際機構驗證且未遭破解之演算法。
	18. 加密金鑰或憑證應定期更換。
系統與服務獲得	19. 執行「源碼掃描」安全檢測。 註：請提供檢測報告及修補紀錄。
	20. 執行「滲透測試」安全檢測。 註：請提供檢測報告及修補紀錄。

備註 1：資通系統使用單一簽入(SSO)進行權限管控，則亦納入檢測範圍

備註 2：依據「資通安全責任等級分級辦法」第十一條，各機關自行或委外開發之資通系統應依「資通系統防護基準」執行控制措施。若因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經等級提交機關或等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

若有不適用之項目，請條列於下方欄並詳細說明。

不適用項目：

表2 「核心資通系統評選表」編號2系統之防護評量表

1.系統環境資訊			
系統名稱		系統等級	<input type="checkbox"/> 高 <input type="checkbox"/> 中 <input type="checkbox"/> 普
系統性質	<input type="checkbox"/> 本地端程式 <input type="checkbox"/> 正式網站 <input type="checkbox"/> 測試網站 <input type="checkbox"/> 正式備援網站 <input type="checkbox"/> 其他：_____		
系統網址	<input type="checkbox"/> 無 <input type="checkbox"/> 有，前台網址為：_____ 後台網址為：_____ 其它網址為：_____		
系統主機服務與埠口 註：將依填寫內容檢測埠口開放狀態，請依現況填寫。	系統主機 IP	開放之埠口	目的原因
	(範例)127.0.0.1	80 443	HTTP HTTPS
	主機 1:		
	主機 2:		
	主機 3:		
多重因素認證	身分驗證是否提供多重因素認證： <input type="checkbox"/> 否 <input type="checkbox"/> 是，請說明登入方式： (範例：帳號密碼 + 簡訊驗證碼) _____ + _____		
連線核心資通系統進行檢測時，「用戶端」須具備條件(可多選)	<input type="checkbox"/> 無特定要求 <input type="checkbox"/> 有(僅支援下列項目，請勾選) 作業系統 <input type="checkbox"/> XP <input type="checkbox"/> Win 7 <input type="checkbox"/> Win 8.x <input type="checkbox"/> Win 10 以上 作業系統位元 <input type="checkbox"/> 32 位元 <input type="checkbox"/> 64 位元 瀏覽器 <input type="checkbox"/> IE8 <input type="checkbox"/> IE9 <input type="checkbox"/> IE10 <input type="checkbox"/> IE11 <input type="checkbox"/> Edge <input type="checkbox"/> Chrome <input type="checkbox"/> FireFox 瀏覽器位元要求 <input type="checkbox"/> 32 位元 <input type="checkbox"/> 64 位元 <input type="checkbox"/> 作業系統必須加入 AD 網域		

	<p>必須使用下列元件：</p> <p><input type="checkbox"/> .NET Framework，版本_____</p> <p><input type="checkbox"/> VC++ Runtime，版本_____</p> <p><input type="checkbox"/> JRE，版本 _____</p> <p><input type="checkbox"/> 必須使用卡片和讀卡機登入</p> <p><input type="checkbox"/> 必須使用自然人憑證登入</p> <p><input type="checkbox"/> 其他，請說明：_____</p>
2. 系統防護評量	
類別	評量項目
普級以上系統適用項目	
識別與鑑別	1. 使用預設密碼登入系統時，應於登入後要求立即變更。
	2. 身分驗證相關資訊不以明文傳輸。
	3. 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。
	註：請說明登入失敗達_____次，鎖定_____分鐘。如前後台設置不一致請分別提供說明。
	4. 使用密碼進行驗證時，應強制最低密碼複雜度。
	5. 密碼變更時，至少不可以與前 3 次使用過之密碼相同。
系統與服務獲得	6. 資通系統應遮蔽鑑別過程中之資訊。
	7. 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。
	8. 執行「弱點掃描」安全檢測。 註：請提供檢測報告及修補紀錄。
	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。

中級以上系統適用項目	
存取控制	10. 採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。
識別與鑑別	11. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。
	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符記。
系統與資訊完整性	13. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。
高級系統適用項目	
存取控制	14. 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。 註：請提供允許閒置時間____分。如前後台設置不一致請分別提供說明。
識別與鑑別	15. 對資通系統之存取採取多重認證技術。
系統與通訊保護	16. 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。
	17. 使用公開、國際機構驗證且未遭破解之演算法。
	18. 加密金鑰或憑證應定期更換。
系統與服務獲得	19. 執行「源碼掃描」安全檢測。 註：請提供檢測報告及修補紀錄
	20. 執行「滲透測試」安全檢測。 註：請提供檢測報告及修補紀錄
備註 1：資通系統使用單一簽入(SSO)進行權限管控，則亦納入檢測範圍 備註 2：依據「資通安全責任等級分級辦法」第十一條，各機關自行或委外開發之資通系統應依「資通系統防護基準」執行控制措施。若因技術限制、個別	

資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經等級提交機關或等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

若有不適用之項目，請條列於下方欄並詳細說明。

不適用項目：

表3 「核心資通系統評選表」編號3系統之防護評量表

1.系統環境資訊			
系統名稱		系統等級	<input type="checkbox"/> 高 <input type="checkbox"/> 中 <input type="checkbox"/> 普
系統性質	<input type="checkbox"/> 本地端程式 <input type="checkbox"/> 正式網站 <input type="checkbox"/> 測試網站 <input type="checkbox"/> 正式備援網站 <input type="checkbox"/> 其他：_____		
系統網址	<input type="checkbox"/> 無 <input type="checkbox"/> 有，前台網址為：_____ 後台網址為：_____ 其它網址為：_____		
系統主機服務與埠口 註：將依填寫內容檢測埠口開放狀態，請依現況填寫。	系統主機 IP	開放之埠口	目的原因
	(範例)127.0.0.1	80 443	HTTP HTTPS
	主機 1:		
	主機 2:		
	主機 3:		
多重因素認證	身分驗證是否提供多重因素認證： <input type="checkbox"/> 否 <input type="checkbox"/> 是，請說明登入方式： (範例：帳號密碼 + 簡訊驗證碼) _____ + _____		
連線核心資通系統進行檢測時，「用戶端」須具備條件(可多選)	<input type="checkbox"/> 無特定要求 <input type="checkbox"/> 有(僅支援下列項目，請勾選) 作業系統 <input type="checkbox"/> XP <input type="checkbox"/> Win 7 <input type="checkbox"/> Win 8.x <input type="checkbox"/> Win 10 以上 作業系統位元 <input type="checkbox"/> 32 位元 <input type="checkbox"/> 64 位元 瀏覽器 <input type="checkbox"/> IE8 <input type="checkbox"/> IE9 <input type="checkbox"/> IE10 <input type="checkbox"/> IE11 <input type="checkbox"/> Edge <input type="checkbox"/> Chrome <input type="checkbox"/> FireFox 瀏覽器位元要求 <input type="checkbox"/> 32 位元 <input type="checkbox"/> 64 位元 <input type="checkbox"/> 作業系統必須加入 AD 網域		

	<p>必須使用下列元件：</p> <p><input type="checkbox"/> .NET Framework，版本_____</p> <p><input type="checkbox"/> VC++ Runtime，版本_____</p> <p><input type="checkbox"/> JRE，版本 _____</p> <p><input type="checkbox"/> 必須使用卡片和讀卡機登入</p> <p><input type="checkbox"/> 必須使用自然人憑證登入</p> <p><input type="checkbox"/> 其他，請說明：_____</p>
2. 系統防護評量	
類別	評量項目
普級以上系統適用項目	
識別與鑑別	1. 使用預設密碼登入系統時，應於登入後要求立即變更。
	2. 身分驗證相關資訊不以明文傳輸。
	3. 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。 註：請說明登入失敗達_____次，鎖定_____分鐘。如前後台設置不一致請分別提供說明。
	4. 使用密碼進行驗證時，應強制最低密碼複雜度。
	5. 密碼變更時，至少不可以與前 3 次使用過之密碼相同。
	6. 資通系統應遮蔽鑑別過程中之資訊。
系統與服務獲得	7. 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。
	8. 執行「弱點掃描」安全檢測。 註：請提供檢測報告及修補紀錄。
	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。

中級以上系統適用項目	
存取控制	10. 採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。
識別與鑑別	11. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。
	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符記。
系統與資訊完整性	13. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。
高級系統適用項目	
存取控制	14. 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。 註：請提供允許閒置時間____分。如前後台設置不一致請分別提供說明。
識別與鑑別	15. 對資通系統之存取採取多重認證技術。
系統與通訊保護	16. 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。
	17. 使用公開、國際機構驗證且未遭破解之演算法。
	18. 加密金鑰或憑證應定期更換。
系統與服務獲得	19. 執行「源碼掃描」安全檢測。 註：請提供檢測報告及修補紀錄。
	20. 執行「滲透測試」安全檢測。 註：請提供檢測報告及修補紀錄。
備註 1：資通系統使用單一簽入(SSO)進行權限管控，則亦納入檢測範圍 備註 2：依據「資通安全責任等級分級辦法」第十一條，各機關自行或委外開發之資通系統應依「資通系統防護基準」執行控制措施。若因技術限制、個別	

資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經等級提交機關或等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。

若有不適用之項目，請條列於下方欄並詳細說明。

不適用項目：