**附件5　核心資通系統安全防護評量表**

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 | | | □高□中□普 |
| 系統性質 | □本地端程式□正式網站□測試網站□正式備援網站  □其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| 系統網址 | □無  □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：  □否  □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) | □無特定要求  □有(僅支援下列項目，請勾選)  　作業系統 □XP □Win 7 □Win 8.x □Win 10以上  　作業系統位元 □32位元 □64位元  　瀏覽器□IE8□IE9□IE10□IE11□Edge□Chrome□FireFox  　瀏覽器位元要求□32位元□64位元  　□作業系統必須加入AD網域  　必須使用下列元件：  　□.NET Framework，版本  　□VC++ Runtime，版本  　□JRE，版本  　□必須使用卡片和讀卡機登入  　□必須使用自然人憑證登入  　□其他，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| 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。 | | | | |
| 1. 身分驗證相關資訊不以明文傳輸。 | | | | |
| 1. 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。 | | | | |
| 1. 使用密碼進行驗證時，應強制最低密碼複雜度。 | | | | |
| 1. 密碼變更時，至少不可以與前3次使用過之密碼相同。 | | | | |
| 1. 資通系統應遮蔽鑑別過程中之資訊。 | | | | |
| 系統與服務獲得 | | 1. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 | | | | |
| 1. 執行「弱點掃描」安全檢測。   註：請提供檢測報告及修補紀錄。 | | | | |
| 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。 | | | | |
| 中級以上系統適用項目 | | | | | | |
| 存取控制 | | 1. 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 | | 1. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 | | | | |
| 1. 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 | | 1. 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 | | 1. 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 | | 1. 對資通系統之存取採取多重認證技術。 | | | | |
| 系統與通訊保護 | | 1. 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。 | | | | |
| 1. 使用公開、國際機構驗證且未遭破解之演算法。 | | | | |
| 1. 加密金鑰或憑證應定期更換。 | | | | |
| 系統與服務獲得 | | 1. 執行「源碼掃描」安全檢測。   註：請提供檢測報告及修補紀錄。 | | | | |
| 1. 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： | | | | | | |

1. 「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 | | | □高□中□普 |
| 系統性質 | □本地端程式□正式網站□測試網站□正式備援網站  □其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| 系統網址 | □無  □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：  □否  □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) | □無特定要求  □有(僅支援下列項目，請勾選)  　作業系統 □XP □Win 7 □Win 8.x □Win 10以上  　作業系統位元 □32位元 □64位元  　瀏覽器□IE8□IE9□IE10□IE11□Edge□Chrome□FireFox  　瀏覽器位元要求□32位元□64位元  　□作業系統必須加入AD網域  　必須使用下列元件：  　□.NET Framework，版本  　□VC++ Runtime，版本  　□JRE，版本  　□必須使用卡片和讀卡機登入  　□必須使用自然人憑證登入  　□其他，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| 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。 | | | | |
| 1. 身分驗證相關資訊不以明文傳輸。 | | | | |
| 1. 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。 | | | | |
| 1. 使用密碼進行驗證時，應強制最低密碼複雜度。 | | | | |
| 1. 密碼變更時，至少不可以與前3次使用過之密碼相同。 | | | | |
| 1. 資通系統應遮蔽鑑別過程中之資訊。 | | | | |
| 系統與服務獲得 | | 1. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 | | | | |
| 1. 執行「弱點掃描」安全檢測。   註：請提供檢測報告及修補紀錄。 | | | | |
| 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。 | | | | |
| 中級以上系統適用項目 | | | | | | |
| 存取控制 | | 1. 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 | | 1. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 | | | | |
| 1. 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 | | 1. 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 | | 1. 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 | | 1. 對資通系統之存取採取多重認證技術。 | | | | |
| 系統與通訊保護 | | 1. 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。 | | | | |
| 1. 使用公開、國際機構驗證且未遭破解之演算法。 | | | | |
| 1. 加密金鑰或憑證應定期更換。 | | | | |
| 系統與服務獲得 | | 1. 執行「源碼掃描」安全檢測。   註：請提供檢測報告及修補紀錄 | | | | |
| 1. 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： | | | | | | |

1. 「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 | | | □高□中□普 |
| 系統性質 | □本地端程式□正式網站□測試網站□正式備援網站  □其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| 系統網址 | □無  □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：  □否  □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) | □無特定要求  □有(僅支援下列項目，請勾選)  　作業系統 □XP □Win 7 □Win 8.x □Win 10以上  　作業系統位元 □32位元 □64位元  　瀏覽器□IE8□IE9□IE10□IE11□Edge□Chrome□FireFox  　瀏覽器位元要求□32位元□64位元  　□作業系統必須加入AD網域  　必須使用下列元件：  　□.NET Framework，版本  　□VC++ Runtime，版本  　□JRE，版本  　□必須使用卡片和讀卡機登入  　□必須使用自然人憑證登入  　□其他，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| 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。 | | | | |
| 1. 身分驗證相關資訊不以明文傳輸。 | | | | |
| 1. 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。 | | | | |
| 1. 使用密碼進行驗證時，應強制最低密碼複雜度。 | | | | |
| 1. 密碼變更時，至少不可以與前3次使用過之密碼相同。 | | | | |
| 1. 資通系統應遮蔽鑑別過程中之資訊。 | | | | |
| 系統與服務獲得 | | 1. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 | | | | |
| 1. 執行「弱點掃描」安全檢測。   註：請提供檢測報告及修補紀錄。 | | | | |
| 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。 | | | | |
| 中級以上系統適用項目 | | | | | | |
| 存取控制 | | 1. 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 | | 1. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 | | | | |
| 1. 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 | | 1. 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 | | 1. 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 | | 1. 對資通系統之存取採取多重認證技術。 | | | | |
| 系統與通訊保護 | | 1. 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。 | | | | |
| 1. 使用公開、國際機構驗證且未遭破解之演算法。 | | | | |
| 1. 加密金鑰或憑證應定期更換。 | | | | |
| 系統與服務獲得 | | 1. 執行「源碼掃描」安全檢測。   註：請提供檢測報告及修補紀錄。 | | | | |
| 1. 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： | | | | | | |