**《機關名》**

**資通安全維護計畫實施情形自評表-C級機關**

| 稽核項目 | 稽核結果 | 佐證資料 |
| --- | --- | --- |
| 符合 | 不符合 |
| 1.核心業務及其重要性 | 1.1核心業務及重要性盤點  |  |  | 核心業務來源(例：組織法) |
| 2.資通安全政策及目標之訂定 | 2.1資通安全政策訂定及核定  |  |  | 資通安全政策 |
| 2.2資通安全目標之訂定  |  |  | 資通安全年度KPI |
| 2.3資通安全政策及目標宣導  |  |  | 函知各單位、會議宣導、網站公告、教育訓練、辦理測驗、E-mail等 |
| 2.4資通安全政策及目標定期檢視 |  |  | 管審會會議資料，資安政策之檢視。 |
| 3.設置資通安全推動組織 | 3.1設定資通安全長及資通安全推動小組 |  |  | 資通安全組織及資通安全組織成員表 |
| 3.2資通安全組織運作 |  |  | 資通安全委員會或管審會簽到單(資安長參加會議次數) |
| 4.專責人力及經費之配置 | 4.1專職(責)人員配置 |  |  | 呈報署內專職(責)人員公文、附表1-資安專責人力表 |
| 4.2經費之配置 |  |  | 附表2-經費配置表(近三年) |
| 5.資訊資產盤點暨風險評估作業 | 5.1資通系統及資訊之盤點及核心資通系統、相關資產之標示 |  |  | 附表3-資訊資產盤點表 |
| 5.2資通安全風險評估及因應  |  |  | 附表4-威脅弱點評估表附表5-風險評鑑彙整表附表6-風險改善計劃表 |
| 6.資通安全防護及控制措施 | 6.1資通安全防護及控制措施 |  |  | 實體安全管理程序書、存取控制管理程序書、通訊與作業管理程序書、系統開發及維護管理程序書。 |
| 7.資通安全事件通報、應變及演練相關機制 | 7.1訂定資通安全事件通報、應變及演練相關機制 |  |  | 資通安全事件通報及應變管理程序 |
| 7.2資通安全事件通報、應變及演練 |  |  | 1.資安事件通報：教育機構資安通報平臺113年資料2.113年通報應變演練：演練證明(演練平臺通報資料、簡訊、Email等)3.社交工程演練紀錄及改善情形4.附表7-社交工程演練結果統計表 |
| 8.資通安全情資之評估及因應機制 | 8.1資通安全情資之評估及因應措施  |  |  | 收到情資項目可進行網頁公告、全機關轉信等，並對於機關可能面臨之情資狀況應進行分析評估並留存紀錄。 |
| 9.資通系統或服務委外辦理之管理 | 9.1選任受託者應注意事項  |  |  | 提供系統委外服務案RFP或廠商服務建議書(含委外廠商之資安能力要求項目、附表8-委外廠商資安管理作業自評表)。 另請針對以下項目自我檢核：1.應符合資安法施行細則第四條之受託者(委外廠商)應具備與應提供事項，如資安專業人員、資安管理措施或第三方驗證。2.系統上線之安全檢測證明。3.應與廠商約定委外系統適用之防護基準。4.應與廠商約定維護水準，如保證系統的完修時間，符合資安維護計畫中的最大容忍中斷時間，備份週期符合系統 RPO。5.應依資安維護計畫，落實委外廠商與人員簽署保密協議。6.應將軟體開發生命週期之各階段安全要求納入合約。7.應將委外關係結束後之資料返還、刪除與保密責任列入合約要求中。8.應約定受委託廠商，知悉資安事件的通報與應變處理責任。 |
| 9.2監督受託者資通安全維護情形應注意事項 |  |  | 提供校務行政(含學習歷程)系統外之委外廠商定期維護紀錄或委外廠商自我檢核表如：附表9-委外廠商查核暨自我檢核項目表，於管理審查階段說明及討論，且應包含維護作業中之資安項目及議題。自我檢核內容同9.1。 |
| 9.3是否辦理委外廠商查核？ |  |  | 1.提供校務行政(含學習歷程)系統外之委外廠商自我檢核表如：附表9-委外廠商查核暨自我檢核項目表2.應於委外廠商查核作業後落實追蹤改善要求，並於管理審查會議說明。3.委外廠商如已通過ISO27001等資訊安全管理系統標準驗證，可請廠商提供相關證明文件。 |
| 10.公務機關所屬人員辦理業務涉及資通安全事項之考核機制 | 10.1訂定考核機制並進行考核 |  |  | 1.機關相關獎懲法規。2.113年機關相關人員奬懲。 |
| 11.資通安全維護計畫及實施情形之持續精進及績效管理機制 | 11.1資通安全維護計畫實施情形之稽核機制 |  |  | 年度稽核計畫、稽核查檢表、稽核報告書、最近1次之實地稽核訪視及書面審查紀錄、管理審查會議紀錄(含追蹤改善情形)。 |
| 11.2資通安全維護計畫之持續精進及績效管理 |  |  | 矯正預防處理單、管理審查會議紀錄(含說明資通安全維護計畫之持續精進及績效管理執行情形)。 |
| 12.管理面 | 12.1資通系統分級及防護基準 |  |  | 附表3-資訊資產盤點表 |
| 12.2資訊安全管理系統之導入 |  |  | 足以證明機關持續導入資通安全管理系統之文件 |
| 12.3資通安全專責人員 |  |  | 同4.1附表1-資安專責人力表 |
| 12.4內部資通安全稽核 |  |  | 同11.1(二年一次) |
| 12.5業務持續運作演練 |  |  | 業務持續運作演練紀錄 |
| 13.技術面 | 安全性檢測 | 13.1弱點掃描 |  |  | 核心系統弱點掃描紀錄(主機及系統皆要做弱點掃描，初測跟複測皆需要繳交)(二年一次) |
| 13.2滲透測試 |  |  | 核心系統滲透測試紀錄(主機及網頁皆要做滲透測試，初測跟復測皆需要繳交)(二年一次) |
| 資通安全健診 | 13.3網路架構檢視 |  |  | 資通安全健診網路架構檢視報告(資通安全健診報告跟修補證明，二年一次) |
| 13.4網路惡意活動檢視 |  |  | 資通安全健診網路惡意活動檢視報告(二年一次) |
| 13.5使用者端電腦惡意活動檢視 |  |  | 資通安全健診使用者端電腦惡意活動檢視報告(二年一次) |
| 13.6伺服器主機惡意活動檢視 |  |  | 資通安全健診伺服器主機惡意活動檢視報告(二年一次) |
| 13.7目錄伺服器設定檢視 |  |  | 資通安全健診目錄伺服器設定檢視報告(二年一次) |
| 13.8防火牆連線設定檢視 |  |  | 資通安全健診防火牆連線設定檢視報告(二年一次) |
| 13.9資通安全弱點通報機制 |  |  | 1.廠商導入作業契約2.截行政院資通安全弱點通報系統(VANS)資訊資產上傳平台圖 |
| 資通安全防護 | 13.10防毒軟體 |  |  | 軟體授權(截圖) |
| 13.11網路防火牆 |  |  | 軟體或硬體、防火牆管理介面證明(截圖) |
| 13.12具有郵件伺服器者，應備電子郵件過濾機制 |  |  | 過濾機制或經授權之軟體硬體(截圖)。 |
| 14.認知與訓練 | 資通安全教育訓練 | 14.1資通安全專責人員 |  |  | 附表10-資通安全教育訓練統計表 |
| 14.2資通安全專責人員以外之資訊人員 |  |  | 附表10-資通安全教育訓練統計表 |
| 14.3一般使用者及主管 |  |  | 附表10-資通安全教育訓練統計表 |

1.附表1-資安專責人力表

2.附表2-經費配置表

3.附表3-資訊資產盤點表

4.附表4-威脅弱點評估表

5.附表5-風險評鑑彙整表

6.附表6-風險改善計劃表

7.附表7-社交工程演練結果統計表

8.附表8-委外廠商資安管理作業自評表

9.附表9-委外廠商查核暨自我檢核項目表

10.附表10-資通安全教育訓練統計表

11.有關技術面13.7及13.12，若機關無相應設備，請勾選「符合」，並於佐證資料欄位中註明無此設備。

備註：附表1至3可依「臺教國署資字第1140034117號」函所提供之附件填寫後檢附。

附表4至10如機關有相對應表單可依機關原表單提出佐證。

# 《機關名》威脅弱點評估表

| 資產編號 | 資產類別 | 資產名稱 | 資產價值 | 威脅 | 弱點 | 威脅等級（發生之可能性）低(1) 中(2) 高(3) | 弱點等級（受到威脅利用之容易度）低(1) 中(2) 高(3) | 風險值 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

備註：1.資產價值：機密性C,完整性I,可用性A取最大值，值為1-4 2.風險值：資產價值＊威脅等級＊弱點等級

承辦人 資安官(資安執行祕書) 資安長

# 《機關名》風險評鑑彙整表

| 項次 | 資產編號 | 資產類別 | 資產名稱 | 資產說明 | 權責單位 | 資產價值 | 風險事件 | 風險值 | 風險再評估 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 威脅 | 弱點 | 資產價值 | 威脅等級 | 弱點等級 | 風險值 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

承辦人 資安官(資安執行祕書) 資安長

**《機關名》****風險改善計劃表**

| 項次 | 現況說明 | 風險改善建議措施 | 教育體系資通安全管理規範條文 | 建議權責單位 | 預計改善時間與處理方式 | 與之風險評估彙整表對照編號 |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

承辦人 資安官(資安執行祕書) 資安長

《機關名》社交工程演練結果統計表

|  |  |  |  |
| --- | --- | --- | --- |
| 演練期別 | 社交工程郵件開啟率 | 社交工程 郵件 連結點閱率 | 社交工程 郵件 附件開啟率 |
| 113年上半年 |  |  |  |
| 113年下半年 |  |  |  |

承辦人 資安官(資安執行祕書) 資安長

《機關名》委外廠商資安管理作業自評表

填表日期： 年 月 日

|  |  |  |  |
| --- | --- | --- | --- |
| **委外廠商名稱** |  | **委外廠商****負責人** |  |
| **專案名稱** |  | **單位/專案負責人** |  |
| **評估項目** | **辦理情形** |
| 1.管理面 |
| 1.1辦理本專案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證 | □辦理本專案受託業務之相關程序及環境已(將)通過\_\_\_\_\_認(驗)證並持續有效，驗證公司為\_\_\_\_\_□辦理本專案受託業務之相關程序及環境已具備完善資安管理措施，詳\_\_\_\_\_文件(如未載明於既有文件內，請於備註欄內說明相關措施)□本專案受託業務之相關程序及環境未導入適當資安管理措施備註：\_\_\_\_\_\_\_\_\_\_ |
| 1.2本專案之資安負責人、資安專責主管或其他資安人員之人力配置規劃 | □本專案之資安負責人(專案主管)為\_\_\_\_□本專案之資安人員為\_\_\_\_□本專案未指派資安負責人、資安專責主管或其他資安人員備註：\_\_\_\_\_\_\_\_\_\_ |
| 1.3本專案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施 | □本專案受託業務相關程序及環境之資安風險評估結果已(將)載明於\_\_\_\_文件，已(將)採取對應之控制措施詳\_\_\_\_文件(如未載明於既有文件內，請於備註欄內說明相關措施)□未就本專案進行資安風險評估備註：\_\_\_\_\_\_\_\_\_\_ |
| 1.4本專案範圍內之資安事件通報應變程序，包含知悉資安事件發生或有發生之虞之相關通報時效規定、通報方式、資安事件調查、處理及改善流程 | □本專案受託業務相關程序及環境之資安事件通報應變程序已(將)載明於\_\_\_\_\_文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資安事件或發現有事件發生之虞時，應於\_\_小時內向甲方等相關利害關係人通報，通報對象包含\_\_\_\_□未就本專案訂定相關資安事件通報及應變程序備註：\_\_\_\_\_\_\_\_\_\_ |
| 1.5由招標公告日起算，過去3年是否發生因管理議題肇因之重大資安事件 | □過去3年無發生因管理議題肇因之資安事件□是，共\_\_次，事件發生主要根因為\_\_\_\_備註：\_\_\_\_\_\_\_\_\_\_ |
| 2.技術面 |
| 2.1本專案範圍內之資通系統，包含主要履約標的之資通系統及其他執行本專案業務所需使用之業務、行政相關資通系統，辦理安全性檢測 | □本專案範圍內之資通系統將規劃執行\_\_\_\_\_(如源碼掃描、弱點掃描、滲透測試)，檢測項目及本案範圍為：\_\_\_\_\_□未就本專案範圍內之資通系統規劃安全性檢測備註：\_\_\_\_\_\_\_\_\_\_ |
| 2.2辦理本專案受託業務環境及設備導入之相關資通安全防護措施 | □本專案受託業務之環境及設備已(將)導入(啟用)\_\_\_\_\_(如防毒軟體、防火牆、電子郵件過濾機制、入侵偵測及防禦機制等)，導入項目及本案範圍為：\_\_\_\_\_□本專案受託業務之環境及設備未導入相關資通安全防護措施備註：\_\_\_\_\_\_\_\_\_\_ |
| 2.3本專案範圍內之資通系統及專案資料之存取控制等權限管理機制，如PM、系統管理員、一般使用者帳號之權限分級原則及控管方式 | □本專案範圍內之資通系統帳號或使用者權限分成\_\_種等級，相關存取控制、權限管理機制說明如下：\_\_\_\_□未規劃本專案範圍內之資通系統及專案資料相關存取控制及權限管理機制備註：\_\_\_\_\_\_\_\_\_\_ |
| 3.認知訓練面 |
| 3.1本專案直接履約相關人員之資安教育訓練 | □本專案直接履約相關人員之資安教育訓練包含\_\_小時之資安通識教育訓練，對象包含\_\_\_\_；\_\_小時之資安專業教育訓練，對象包含\_\_\_\_□未規劃相關資安教育訓練備註：\_\_\_\_\_\_\_\_\_\_ |
| 3.2本專案團隊人員取得之資通安全專業證照 | □本專案具資安證照之團隊成員有：\_\_位□本專案團隊人員未具備資通安全專業證照備註：\_\_\_\_\_\_\_\_\_\_ |

廠商用印：

《機關名》委外廠商查核暨自我檢核項目表

查核人員： 填表日期：年月日

|  |  |  |  |
| --- | --- | --- | --- |
| **查核項目** | **查核內容** | **查核結果** | **說明** |
| **符合** | **不符****合** | **不適****用** |
| **1.資通安全責任** | 1.1 是否知悉甲方資通安全責任等級？ | **□** | **□** | **□** |  |
| 1.2 是否是否知悉合約標的之系統防護基準？ | **□** | **□** | **□** |  |
| 1.3 是否了解甲方資安維護計畫對合約標的系統各項要求？ | **□** | **□** | **□** |  |
| **2.應辦事項** | 2.1 系統是否符合防護基準？ | **□** | **□** | **□** |  |
| 2.2 系統是否具備合適備份機制？ | **□** | **□** | **□** |  |
| 2.3 是否完成系統弱掃，並完成修補中級(含)以上之風險？ | **□** | **□** | **□** |  |
| 2.4 是否完成資通安全健診，並完成修補中級(含)以上之風險？ | **□** | **□** | **□** |  |
| 2.5 是否完成滲透測試，並完成修補中級(含)以上之風險？ | **□** | **□** | **□** |  |
| 2.6 是否完成源碼檢測，並完成修補中級(含)以上之風險？ | **□** | **□** | **□** |  |
| 2.7 是否實施之系統日誌管理？ | **□** | **□** | **□** |  |
| 2.8 是否配合甲方每年辦理1次業務持續運作演練及1次資通安全事件通報演練？ | **□** | **□** | **□** |  |
| 2.9 是否參加3小時以上資通安全通識教育訓練及3小時以上資通安全專業課程訓練或資通安全職能訓練？ | **□** | **□** | **□** |  |
| **3.資安風險處理及預防措施** | 3.1 是否有符合人員及設備安全評估措施？ | **□** | **□** | **□** | □人員不得為陸籍□設備不得為大陸品牌 |
| 3.2 是否簽署廠商保密同意書、廠商執行人員保密切結書 | **□** | **□** | **□** | □廠商保密同意書□執行人員保密切結書 |
| 3.3 作業環境是否進行合適控管？□具 ISO27001認證□不具 ISO27001認證 | **□** | **□** | **□** | □進行資通系統盤點□進行資通系統風險評估□有防火牆且有管控規則□有日誌管理□有合適權限管控 |

廠商名稱、住址及公司章：

《機關名》資通安全教育訓練統計表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 人員類別 | 應完成資通安全教育訓練時數(時/人) | 機關人數 | 完成人數 | 完成百分比 |
| 資通安全專責人員 | 12 |  |  |  |
| 資通安全專責人員以外之資訊人員 | 3小時/年(通識)+3小時/二年(專業) |  |  |  |
| 一般使用者及主管 | 3 |  |  |  |

備註：依資通安全管理法常見問題，資訊人員泛指機關資訊單位所屬人員，或業務單位所屬人員並從事資通系統自行或委外設置、開發、維運者。例如：系統管理者、系統承辦人、擁有系統後台管理權限之人員等

承辦人 資安官(資安執行祕書) 資安長