**資通安全維護計畫實施情形檢核表(範本)**

附件1

OO：請機關依自身情形填入內容；小括弧()：為備註說明；中括弧[]：為選用文字

|  |  |  |
| --- | --- | --- |
| 實施項目 | 實施內容 | 辦理情形(填寫範例) |
| 1. 核心業務及其重要性 | 1. 核心業務及重要性盤點 | 依資安法施行細則第七條規定，本機關已[將]落實機關核心業務及核心資通系統之界定，盤點核心業務及重要性，108年核心業務計O項，並已[將]敘明於109年維護計畫中。 |
| 1. 資通安全政策及目標之訂定 | 1. 資通安全政策訂定及核定 | 本機關108年資通安全政策已訂定於OOO文件(編號、名稱及章節)內，係經本機關首長[資安長|OOO]核定，並已[將]敘明於109年維護計畫中。 |
| 1. 資通安全目標之訂定 | 本機關資通安全目標已訂定於OOO文件(編號、名稱及章節)內，並已[將]敘明於109年維護計畫中。 |
| 1. 資通安全政策及目標宣導 | 本機關108年資通安全政策及目標，已定期向同仁及利害關係人進行宣逹，宣導方式包含函知各單位、文件放置網站、教育訓練及OOO等。 |
| 1. 資通安全政策及目標定期檢視 | 本機關於OOO會議中定期檢討資通安全政策及目標，108年計檢視O次。 |
| 1. 設置資通安全推動組織 | 1. 設定資通安全長 | 本機關108年已指定OOO(姓名及職稱)為資通安全長，其職掌已訂於OOO文件(編號、名稱及章節)內。 |
| 1. 設置資通安全推動小組 | 本機關108年已設置資通安全推動小組，由OOO(姓名及職稱)擔任召集人，包含O個機關單位共O人，各單位成員層級為OO以上，其運作及成員職掌已訂於OOO文件(編號、名稱及章節)內。  108年召開O次小組會議，會議日期為O年O月O日、O月O日，由OOO主持，成員親自出席比例為OO%。 |
| 1. 專責人力及經費之配置 | 1. 專職(責)人員配置 | 本機關108年依規定配置資通安全專責人員O人，其中專職人員O人，已具備資通安全專業證照O張及資通安全職能評量證書O張，詳如附表1。 |
| 1. 經費之配置 | 本機關已視需求合理分資安經費，108年資安經費佔資訊經費之O% ，詳如附表2。 |
| 1. 資訊及資通系統之盤點及核心資通系統、相關資產之標示 | 1. 資訊及資通系統之盤點 | 本機關已於O年O月完成資訊及資通系統盤點，並建立本機關之資訊資產清冊[OOO文件(編號、名稱及章節)]內，計有O筆資產。其中資通系統(含OT)如附表3，大陸品牌資通訊設備清冊如附表4。 |
| 1. 機關資通安全責任等級分級 | 本機關依資通安全責任等級分級辦法，被核定為資通安全責任等級O級機關。 |
| 1. 資通安全風險評估 | 1. 資通安全風險評估 | 本機關已於O年O月完成本機關之資訊、資通系統及相關資產之風險分析評估，其評估方式及評估結果已敘明於OOO文件(編號、名稱及章節)內。  物聯網設備已[部分|尚未]納入前述作業，預計O年O月前納入。 |
| 1. 資通安全風險之因應 | 本機關針對風險評估結果已擬定對應之資通安全防護及控制措施，並敘明於OOO文件(編號、名稱及章節)內，已[預定於O年O月前]完成防護及控制措施。  物聯網設備已[部分|尚未]納入前述作業，預計O年O月前納入。 |
| 1. 資通安全防護及控制措施 | 1. 資通安全防護及控制措施 | 本機關資通安全防護及控制措施已訂定於OOO文件(編號、名稱及章節)內，並已納入資通安全責任等級分級辦法相關規定，執行情形載明於OOO文件(編號、名稱及章節)，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核其執行情形，108年未發現有未落實情形[發現OOO有未落實情形，其情形為…，預計O年O月前完成改善]。 |
| 1. 資訊及資通系統之保管 | 本機關已依風險評估結果、自身責任等級應辦事項及核心資通系統防護基準，採行相關防護控制措施，詳參資通安全維護計畫。 |
| 1. 存取控制與加密機制管理 | 本機關存取控制與加密機制管理機制已訂定於OO文件(編號、名稱及章節)內，並已納入資通安全責任等級分級辦法相關規定，執行情形載明於OO文件(編號、名稱及章節)，並透過OOO (管審/專案會議、稽核或其他方式)定期檢核其執行情形，108年未發現有未落實情形[發現OOO有未落實情形，其情形為…，預計O年O月前完成改善]。 |
| 1. 作業及通訊安全管理 | 本機關作業及通訊安全管理機制已訂定於OO文件(編號、名稱及章節)內，並已納入資通安全責任等級分級辦法相關規定，執行情形載明於OO文件(編號、名稱及章節)，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核其執行情形，108年未發現有未落實情形[發現OOO有未落實情形，其情形為…，預計O年O月前完成改善]。 |
| 1. 系統獲取、開發及維護 | 本機關系統獲取、開發及維護機制已訂定於OOO文件(編號、名稱及章節)內，並已納入資通安全責任等級分級辦法相關規定，執行情形載明於OOO文件(編號、名稱及章節)，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核其執行情形，108年未發現有未落實情形[發現OOO有未落實情形，其情形為…，預計O年O月前完成改善]。 |
| 1. 業務持續運作演練 | 本機關業務持續運作演練機制已訂定於OOO文件(編號、名稱及章節)內，並已納入資通安全責任等級分級辦法相關規定，執行情形載明於OOO文件(編號、名稱及章節)，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核其執行情形，108年未發現有未落實情形[發現OOO有未落實情形，其情形為…，預計O年O月前完成改善]。 |
| 1. 執行資通安全健診 | 本機關資通安全健診作業已訂定於OOO文件(編號、名稱及章節)內，並已納入資通安全責任等級分級辦法相關規定，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核其執行情形，108年執行情形提報於資通安全管理法應辦事項之辦理現況。 |
| 1. 資通安全防護設備 | 本機關資通安全防護設備已[部分設備|尚未]依資通安全責任等級分級辦法相關規定建置，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核其執行情形，108年執行情形提報於資通安全管理法應辦事項之辦理現況。 |
| 1. 資通安全事件通報、應變及演練相關機制 | 1. 訂定資通安全事件通報、應變及演練相關機制 | 本機關資通安全事件通報、應變及演練相關機制已訂定於OOO文件(編號、名稱及章節)內，並已納入資通安全責任等級分級辦法相關規定，執行情形載明於OOO文件(編號、名稱及章節)，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核其執行情形。 |
| 1. 資通安全事件通報、應變及演練 | 1. 資安事件通報：本機關108年計通報O級事件O件，皆於規定期限內通報[其中O件逾限通報]；所屬機關計通報O級事件O件，皆於規定期限內完成審核[其中O件逾限審核]。 2. 108年攻防演練：整體作業於O年O月O日完成，並於完成後1個月[O個月]內提報執行情形及成果報告交主管機關。 3. 社交工程演練：於O年O月、O月辦理O次，計OO個參與機關，點閱率OO%，開啟率OO%。 4. 通報應變演練：於O年O月O月辦理O次，計O個機關逾限通報。 |
| 1. 資通安全情資之評估及因應機制 | 1. 資通安全情資之分類評估 | 本機關情資來源計有OOO、OOO、OOO等O個管道。  本機關資通安全情資之分類評估機制已訂定於OOO文件(編號、名稱及章節)內，計有OOO、OOO、OOO等OO個類別。 |
| 1. 資通安全情資之因應措施 | 本機關資通安全情資之因應措施已訂定於OOO文件(編號、名稱及章節)內，執行情形載明於OOO文件(編號、名稱及章節)，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核其執行情形。108年計分享O筆情資，接收O筆情資，接收情資中有進一步處理的計有O筆。 |
| 1. 資通系統或服務委外辦理之管理 | 1. 選任受託者應注意事項 | 本機關資通系統或服務委外，選任受託者應注意事項已[預定]於O年O月O日納入採購招標文件中，包含要求ISMS導入、安全性檢測、稽核其執行等。 |
| 1. 監督受託者資通安全維護情形應注意事項 | 本機關監督受託者資通安全維護情形應注意事項已訂定於OOO文件(編號、名稱及章節)內，已納入資通安全管理法相關規定，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核各專案執行情形。  108年計O份契約，其中O份契約已納入前述規定，其餘契約將於O年O月前納入相關規定。 |
| 1. 資通安全教育訓練 | 1. 資通安全教育訓練要求 | 本機關資通安全教育訓練要求已訂定於OOO文件(編號、名稱及章節)內，並透過OOO(管審/專案會議、稽核或其他方式)定期檢核執行情形。 |
| 1. 辦理資通安全教育訓練 | 本機關108年資通安全教育訓練執行情形提報於資通安全管理法應辦事項之辦理現況。 |
| 1. 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 | 1. 訂定考核機制並進行考核 | 本機關108年資通安全考核情形：  1.獎：共O人，記O。  2.懲：共O人，記O。 |
| 1. 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 | 1. 資通安全維護計畫之實施 | 本機關於導入之ISMS機制內，納入資通安全管理法相關規定[本機關已依規定訂定各階文件、流程、程序或控制措施]，實施並保存相關之執行成果紀錄。 |
| 1. 資通安全維護計畫實施情形之稽核機制 | 本機關稽核機制已訂定於OOO文件(編號、名稱及章節)內，稽核項目已納入資通安全管理法相關規定，執行情形載明於OOO文件(編號、名稱及章節)，並透過OOO(後續追蹤管考機制)定期檢核其執行情形。  本機關內部稽核對象共有O個單位，稽核規劃為每年O個，預於O年內可完成全部單位稽核。  稽核小組成員包含O個單位，共O人，每次稽核成員規劃為…(人數及組成規則)。 |
| 1. 資通安全維護計畫之持續精進及績效管理 | 108年於O月O日、O月O日辦理O次內部稽核，計O個單位受稽，計有O項改善建議，預計於O年O月前完成改善。 |
| 1. 對所屬/所監督/所管機關(構)訂定稽核計畫 | 本機關對所屬/所監督/所管機關(構)訂定稽核計畫已訂定於OOO文件(編號、名稱及章節)內，稽核項目已納入資通安全管理法相關規定，執行情形載明於OOO文件(編號、名稱及章節)，並透過OOO(後續追蹤管考機制)定期檢核執行情形。  本機關所屬/所監督/所管機關共有O個，稽核規劃為每年O個，預於O年內可完成全部機關稽核。  稽核小組成員包含O個單位，共O人，每次稽核成員規劃為…(人數及組成規則)。 |
| 1. 對所屬/所監督/所管機關(構)辦理資通安全維護計畫實施情形之稽核 | 本機關108年已於O年O月辦理O個所屬/所監督/所管機關之稽核作業，計有O項改善建議，預計於O年O月前完成改善。 |
| 其他說明 |  | |

附表1 機關專職人力

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 機關  名稱 | 姓名 | 職稱 | 人員屬性  (職聘僱或委外) | 是否專職 | 持有之有效專業證照張數 | 持有之有效職能評量證書張數 |
| 外交部 | 王OO | 分析師 | 職員 | 是 | 1 | 1 |
| 外交部 | 蔡OO | 管理師 | 職員 | 是 | 2 | 1 |

填表說明：

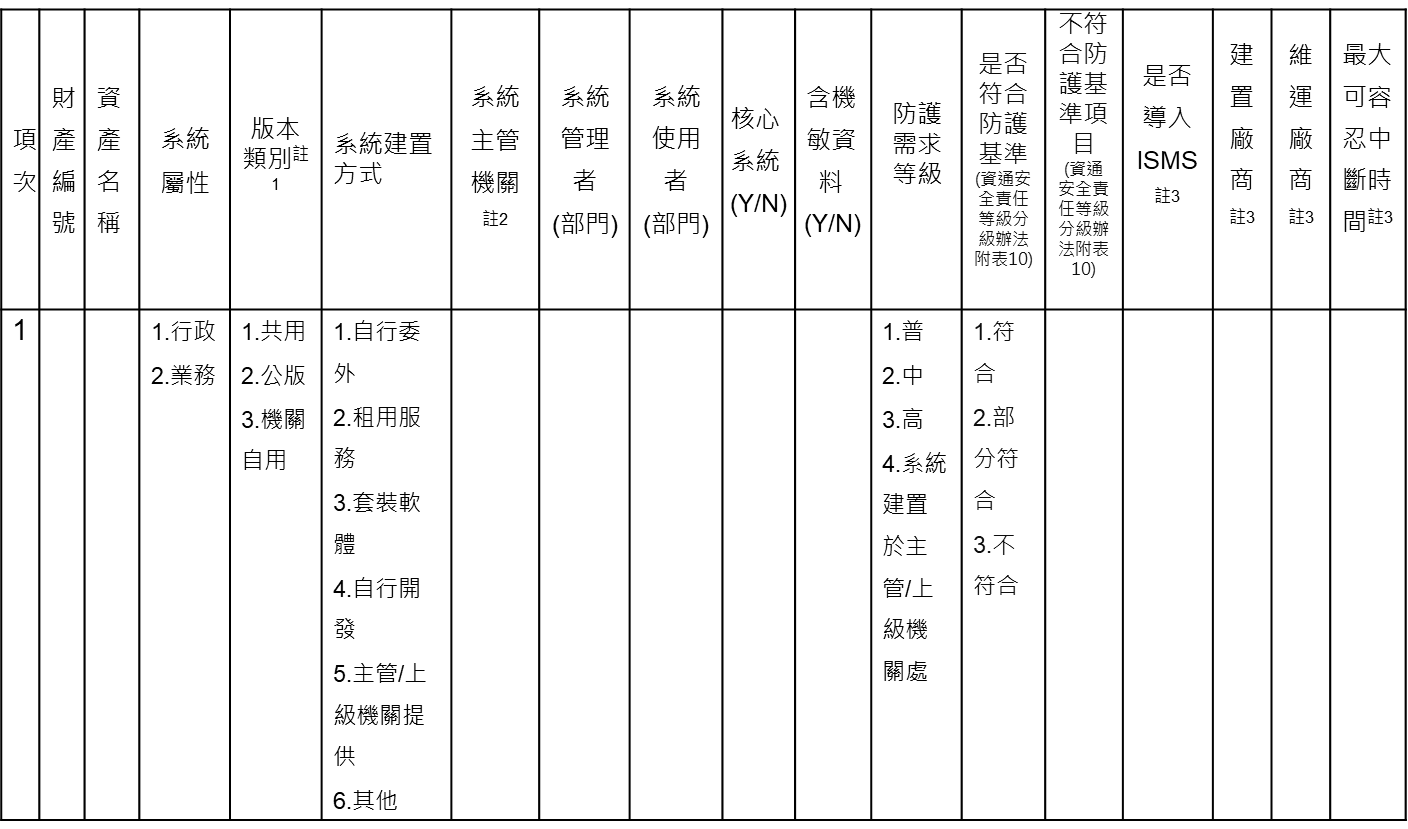
1. 請依機關資安責任等級應具備之資安專職人數進行填寫，即A級機關至少應填4人。
2. 如已有缺額但待聘，姓名欄位請填「待聘」；如尚待爭取員額，職稱欄位請填「待爭取」，其餘欄位不用填。

附表2 經費配置(提報年度，千元)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 機關名稱 | 機關年度經費  -資本門 | 機關年度經費  -經常門 | 年度資訊經費  -資本門 | 年度資訊經費  -經常門 | 年度資安經費  -資本門 | 年度資安經費  -經常門 |
| 外交部 | 1,000,000 | 700,000 | 40,000 | 30,000 | 10,000 | 8,000 |

填表說明：

1. 資訊經費係指各機關之業務費、設備及投資費。
2. 業務費(經常門)：
   * 1. 教育訓練費：凡各機關、學校處理經常一般公務或特定工作計畫所需之各項業務費用屬之。凡對現職員工實施教育訓練所需補貼(補助)有關學分費、雜費、教材、膳宿及交通費等費用屬之。
     2. 資訊服務費：凡公務所需使用資訊操作、維修、購買雲端等服務費用、金額未達1萬元之軟體購置或屬營業租賃性質之資訊設備租金屬之。
3. 設備及投資(資本門)：
4. 資訊軟硬體設備費：凡公務所需各項電腦設施、週邊設備、裝置（含一次購買時所配置之套裝軟體，如作業系統軟體，以及後續2年以上效益之軟體改版、升級與應用系統開發規劃設計）及雲端服務等購置（含資本租賃）費用屬之。
5. 資安經費(經常門、資本門)：辦理資通安全管理法及其子法 之法遵事項相關經費。

附表3 機關資通系統資產清冊

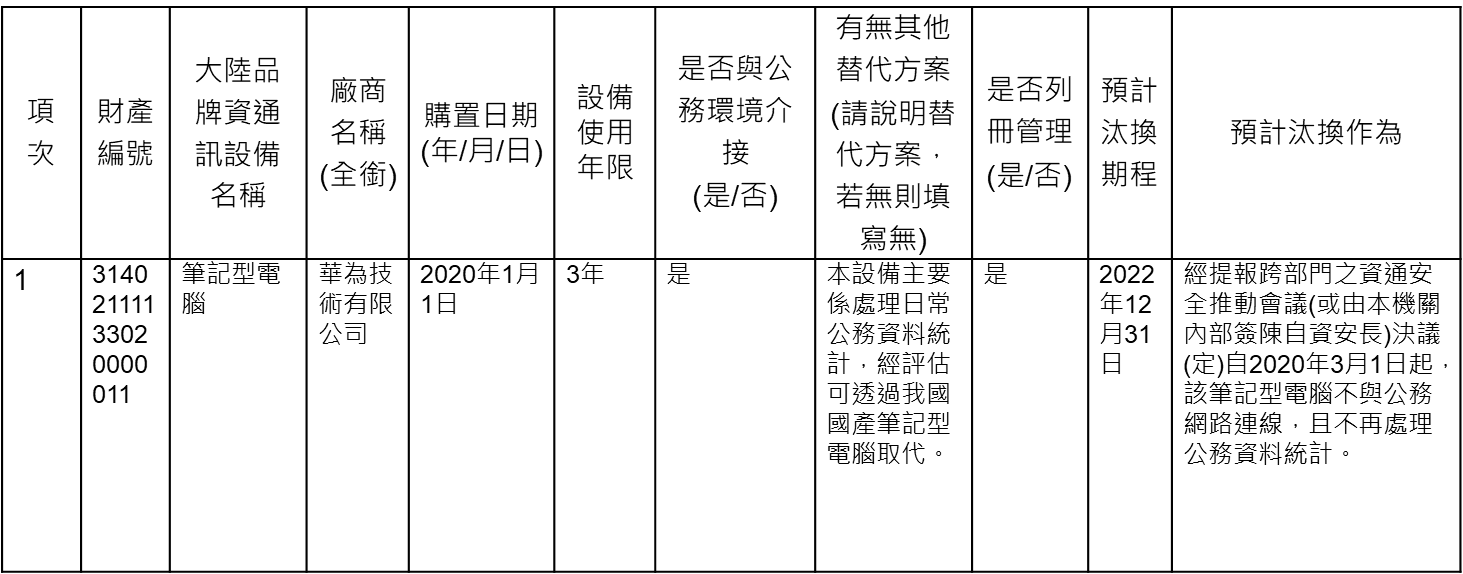
填表說明：

1. 資通系統包含IT(Information Technology)及OT(Operational Technology) ，OT如影像安全控制管理、門禁監控、物聯設備相關管理等系統；其餘資產由機關自行管理
2. 註1：

共用：2個以上機關共同使用之系統 (如戶政、地政、財政、人事差勤系統)。

公版：各機關依特定版本自行維運使用(如公務出國報告資訊網)。

1. 註2：系統建置方式為「5.主管/上級機關提供」，則於此欄位敘明主管/上級機關；若為「6.其他」，請於本欄位說明建置方式；其餘建置方式則免填。
2. 註3：系統建置方式為「5.主管/上級機關提供」得免填。

附表4 大陸品牌資通訊設備清冊

填表說明：

1. 調查大陸品牌資通訊設備(建議由機關財產系統產出)
2. 資通訊設備(參考資通安全管理法第3條用詞定義)：用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之硬體設備。
3. 欄位說明
   * 1. 是否與公務環境介接：是否有連接公務網路或公務設備進行資料傳輸等行為。
     2. 有無其他替代方案：是否有其他國家或我國可替代之產品及方案。
     3. 是否列冊管理：是否定期進行盤點作業，執行該設備之安全性檢測或漏洞修補，並於跨部門之資通安全推動會議提出檢討。
     4. 預計汰換期程：請填寫預計汰換日期(年/月/日)。
     5. 預計汰換作為：請填寫預計汰換作為。