行政院國家資通安全會報111年資通安全作業管考系統填報暨112年實地稽核資料準備說明

國教署資安業務輔導團

國立華南高商　圖書館主任　劉耀明

「111年資通安全維護計畫實施情形」注意事項

- 填寫日期：112年4月7日-112年5月26日
- 應填報項目：【附表1-機關專責人力】、【附表2-經費配置】、【附表 3-機關資通系統與服務資產清冊】、【實施情形檢核表】及【機關應辦事項】，填報項目因各機關資安責任等級不同稍有調整。
- 填報機關：各公務機關(含學校)。

簡報大綱

- 附表1-機關專職人力-填寫
- 附表2-經費配置
- 附表3-機關資通系統與服務資產清冊
- 實施情形檢核表
- 機關應辦事項
- 112年實地查核

附表1-機關專職人力-填寫

- 姓名
- 職稱
- 公務信箱
- 人員屬性(正職、約聘、約僱、委外或約用)
- 是否專職(是/否)
- 負責資安職務之面向(策略面、管理面、技術面)
- 資安專業證照or資安職能證書名稱
- 發證日期*西元年/月/日
- 有效期限*西元年/月/日

附表2-經費配置-填寫

111年機關預算執行：	112年機關預/概算配置(如已審議填預算)：	**111年資安自主產品採購金額**
1. 機關年度經費-資本門	7. 機關年度經費-資本門	111年資通安全硬體產品
2. 機關年度經費-經常門	8. 機關年度經費-經常門	111年資資通安全軟體產品
3. 年度資訊經費-資本門	9. 年度資訊經費-資本門	111年資資通安全服務
4. 年度資訊經費-經常門	10. 年度資訊經費-經常門	
5. 年度資安經費-資本門	11. 年度資安經費-資本門	
6. 年度資安經費-經常門	12. 年度資安經費-經常門	

附表3-機關資通系統與服務資產清冊1

- 財產編號：(非必填)
- 資產名稱(系統名稱)：(必填)
- 系統屬性：(必填，限填「行政」或「業務」、「兼具行政/業務」)
- 系統建置方式：(限填「委外開發」、「租用服務」、「購買套裝軟體」、「自行開發」、「其他」)
- 建置方式補充說明：「系統建置方式」為「其他」者必填

附表3-機關資通系統與服務資產清冊2

- 系統管理者(部門/單位)：(必填)
- 系統使用者(部門/單位)：(必填)
- **系統建置日期(西洋年/月)**
- 主機設置於機關內(是/否)：　(必填，限填「是」或「否」)
- 核心系統(是/否)：(必填，限填「是」或「否」)註：機關之核心系統以應用系統為主
- 含機敏資料(是/否)：(必填，限填「是」或「否」) 機敏資訊以非明文方式儲存(必填，是/否/無機敏資訊/其他機關維運)
- 機敏資訊類別:註:「無機敏資訊」者免填(例如身分證字號、特種個資、稅務資料等)
- 是否與民生權益相關(是/否)：(必填，限填「是」或「否」)註：民生權益係指考試、福利、醫療等
- 防護需求等級：(必填，限填「普」、「中」、「高」、「套裝軟體」)

附表3-機關資通系統與服務資產清冊3

- 是否包含於ISMS導入範圍：（必填，限填「是」或「否」）「系統建置方式」為「主管/上級機關提供」得免填）
- 建置廠商：(必填）系統建置方式為「套裝軟體」者請填「套裝軟體」、若為機關自行開發者，請填寫該機關名
- 建置廠商之統一編號：(必填)註：系統建置方式為「套裝軟體」者請填「2」
- 維運廠商：(必填)註：系統建置方式為「套裝軟體」者請填「套裝軟體」、若為機關自行維運者，請填寫該機關名
- 維運廠商之統一編號：(必填)註：系統建置方式為「套裝軟體」者請填「2」
- 最大可容忍中斷時間(小時)：　（必填，限填整數，不含逗號）
- 是否符合防護基準：（必填，限填「符合」、「部分符合」、「不符合」或「不適用」）
- 不符合防護基準代碼：「是否符合防護基準」為「部分符合」及「不符合」則為必填項目、代碼參「驗證項目代碼」　，多項請以「/」隔開）

資通安全責任等級分級辦法
附表十資通系統防護基準

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
存取控制	帳號管理	一、逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二、應依機關規定之情況及條件，使用資通系統。 三、監控資通系統帳號，如發現帳號違常使用時回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。
	最小權限	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。		無要求。
	遠端存取	一、應監控資通系統遠端連線。 二、資通系統應採用加密機制。 三、資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。 四、等級「普」之所有控制措施。		對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。

附表7-3

代碼	構面	驗證項目
C0101	存取控制	帳號管理
C0102		最小權限
C0103		遠端存取
C0201	事件日誌與可歸責性	記錄事件
C0202		日誌紀錄內容
C0203		日誌儲存容量
C0204		日誌處理失效之回應
C0205		時戳及校時
C0206		日誌資訊之保護

附表7-3

C0301	營運持續計畫	系統備份
C0302		系統備援
C0401	識別與鑑別	內部使用者之識別與鑑別
C0402		身分驗證管理
C0403		鑑別資訊回饋
C0404		加密模組鑑別
C0405		非內部使用者之識別與鑑別

C0501	系統與服務獲得	系統發展生命週期需求階段
C0502		系統發展生命週期設計階段
C0503		系統發展生命週期開發階段
C0504		系統發展生命週期測試階段
C0505		系統發展生命週期部署與維運階段
C0506		系統發展生命週期委外階段
C0507		獲得程序
C0508		系統文件
C0601	系統與通訊保護	傳輸之機密性與完整性
C0602		資料儲存之安全
C0701	系統與資訊完整性	漏洞修復
C0702		資通系統監控
C0703		軟體及資訊完整性

附表3-機關資通系統與服務資產清冊4

- 系統是否對外(必填，是/否)
- 系統日誌保存時間是否超過6個月(必填，是/否)
- 有無開放遠端連線維護(必填，有/無/其他機關維運)
- 是否禁用弱密碼(是/否/不適用/其他機關維運)(必填)
- 是否禁用弱密碼(是/否/不適用)(必填)，

附表3-機關資通系統與服務資產清冊5

- 系統是否備份(是/否)
- 系統是否備妥流量清洗機制(是/否/非對外系統)
- 系統是否備妥CDN啟用作業程序(是/否/非對外系統)
- 系統是否備妥靜態網頁(是/否/非對外系統)
- 系統是否可於10分鐘內切換至靜態網頁(是/否/非對外系統)註：系統是否對外為「否」請填「非對外系統」

附表3機關資通系統與服務資產清冊(使用「主管/上級/其他機關」維運之資通系統)

- 財產編號：(非必填)
- 資產名稱(系統名稱)：(必填)
- 系統屬性：(必填，限填「行政」或「業務」、「兼具行政/業務」)
- 系統主管機關OID：如為共用性系統，請填寫實際維護機關(具備系統設定修改或程式更新等權責)
- 系統主管機關名稱：如為共用性系統，請填寫實際維護機關(具備系統設定修改或程式更新等權責)
- 系統使用者(部門/單位)：(必填)
- 核心系統(是/否)：(必填)機關之核心系統以應用系統為主，並由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

附表3-3資通訊設備清冊

- 設備名稱
- 廠牌名稱
- 數量

1本項調查作業包含個人電腦、筆電、螢幕、印表機等資通設備。

2.調查範圍建議參照行政院主計總處「財物標準分類」之財物編號，至少包含「機械及設備分類明細表」項下之「電腦系統」(分類編號3140101~3140503)各類財產，其餘非屬前開項下之資通設備，例如：遙控無人機(分類編號4030204-06)、手機(分類編號4050202-05)等資通設備亦請納入盤點。

實施情形檢查表1

實施項目	實施內容	辦理情形
1.核心業務及其重要性	1.1核心業務及重要性盤點？ 註：有關核心業務及核心資通系統之定義，請參考資通安全管理法施行細則第7條	○盤點機關核心業務計?項 ○未盤點機關核心業務原因為： 補充說明(選填)：

實施情形檢查表2

實施項目	實施內容	辦理情形
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？ 註：資安政策參考範例如下 1. 符合法令與法規要求 2. 落實資通安全教育訓練，以提高員工之資訊安全意識 3. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅	(單選) O本機關資通安全政策為： O本機關資通安全政策訂定於文件內(編號、名稱及章節)： O未訂定，原因為：_____。 補充說明(選填)：
	2.2 資通安全目標之訂定？ 註：資通安全目標參考範例如下 1. 同仁皆達到資安時數 2. 同仁社交工程點閱及開啟連結率符合要求。	(單選) O本機關資通安全目標為： O本機關資通安全目標訂定於文件內(編號、名稱及章節)： O未訂定，原因為：_____。 補充說明(選填)：
	2.3 資通安全政策及目標宣導？ 註：宣導方式包含：函知各單位、會議宣導、網站公告、教育訓練、辦理測驗等。	(單選) O已向同仁宣導，方式為： O未宣導，原因為：_____。 補充說明(選填)：
	2.4 資通安全政策及目標定期檢視	(單選) 本機關111年資安政策及目標檢視方式為： O於會議中檢視，會議名稱為：　(如管審會、月會、季報、年度會議等) O簽陳主管核定，核定主管為：　(姓名+職稱，如王小明副局長) O未檢視，原因為：_____。 補充說明(選填)：

實施情形檢查表3

實施項目	實施內容	辦理情形
3.設置資通安全推動組織	3.1設定資通安全長	○本機關110年資通安全長為（姓名+職稱，如王小明副局長） ○未設資通安全長(未符法遵），原因為：_____ 補充說明(選填)：
	3.2 設置或加入資通安全推動小組	本機關參與之資安推動組織如下： ○自行簽辦設置，111年計開會?次，本機關資安長親自出席?次。 ○參與其他機關推動組織，主政機關為?，111年計開會?次，本機關資安長親自出席次。 ○無設置且無參加(其他)機關資安推動組織，原因為：_____。 補充說明(選填)：

實施情形檢查表4

實施項目	實施內容	辦理情形
4.專責人力及經費之配置	4.1 專職(責)人員配置	A~C級機關： 本機關總預算員額計___人，資訊人員計人，資安人員配置詳本機關附表一、機關資安人力。 D、E級機關： 本機關總預算員額計___人，資訊人員計人，無須配置資安專職人員，本機關資安相關業務承辦人數為：____人 A~E級機關：補充說明(選填)：
	4.2 經費之配置	附表2-經費配置 補充說明(選填)：

實施情形檢查表5

實施項目	實施內容	辦理情形
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	詳本機關 附表3-資通系統資產清冊 補充說明(選填)：
6. 資通安全風險評估	6.1 資通安全風險評估及因應？ 註：風險評估結果範例：人員共用帳號點選未經識別或不受信任的連結...。 風險之因應範例：提升人員資安意識、敘明於機關資安政策並宣導，以降低風險。	(單選) 〇本機關資安風險評估結果為：__，因應措施為：_____ 。 〇評估結果及因應措施載明於文件內(編號、名稱及章節)： 〇無進行風險評估及因應 補充說明(選填)：

實施情形檢查表6

實施項目	實施內容	辦理情形
7. 資通安全防護及控制措施	7.1 資通安全防護及控制措施	○本機關之資通安全防護及控制措施(含存取控制與加密機制管理、作業及通訊安全管理、系統開發及維護機制、防毒軟體、網路防火牆等)規定於　文件(編號、名稱及章節) ○本機關無資通安全防護及控制措施相關規定文件，原因為: ____。 補充說明(選填)：
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制？ 註：不一定要機關自行訂定，可採用上級機關訂定之資安事件通報機制。	(單選) ○本機關資通安全事件通報、應變及演練相關機制規定於 文件中。 ○本機關遵守上級(其他)機關所訂定之資通安全事件通報、應變及演練相關機制，訂定機關為 ○機關無相關機制(未符法遵) 補充說明(選填)：

實施情形檢查表7

實施項目	實施內容	辦理情形
8.資通安全事件通報、應變及演練相關機制	8.2 資通安全事件通報、應變及演練	1.111年資安事件通報： (單選) O本機關111年計通報資安事件_件，符合相關時限規定。 O本機關111年計通報資安事件_件，有_件事件不符合時限規定。 O無資安事件 補充說明(選填)： 2.111年社交工程演練： (單選) O計 位同仁點閱(點閱率 %)， 位同仁開啟內容連結(開啟連結率 %) O未辦理。原因： O未參與上級(其他)機關所辦理社交工程演練。 補充說明(選填)： 3.111年通報應變演練 (單選) O符合相關時限規定 O有不符合時限規定情形： O未參與上級(其他)機關所辦理通報應變演練。 未辦理 補充說明(選填)：

實施情形檢查表8

9.資通安全情資之評估及因應機制	9.1資通安全情資之評估及因應措施？ 註：資安情資來源如上級機關、技服中心、ISAC等…	(單選) 〇本機關資安情資來源有：　，已進行情資評估及因應措施，情資分類評估機制及因應措施載明於　文件(編號、名稱及章節) 〇本機關資安情資來源有：　，但無資安情資之評估及因應措施相關文件 〇本機關未知悉任何資安情資來源，且無資安情資之評估及因應措施相關文件 原因為：_____。 補充說明(選填)：
10.資通系統或服務委外辦理之管理	10.1選任受託者應注意事項	(單選) 〇本機關無資通系統或服務委外 〇本機關資通系統或服務委外，選任受託者應注意事項(如要求ISMS導入、安全性檢測、稽核其執行等、資安事件通報等)已納入並明確標註於採購招標文件中。 〇本機關有資通系統或服務委外，但未訂定選任受託者應注意事項。 原因為：_____。 補充說明(選填)：
	10.2監督受託者資通安全維護情形應注意事項	(單選) 1.訂定規範或文件： 〇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 _____文件(編號、名稱及章節)內。 〇本機關無資通系統或服務委外 〇未訂定監督受託者資通安全維護情形應注意事項，原因為：_____ 補充說明(選填)：

實施情形檢查表9

實施項目	實施內容	辦理情形
	10.2監督受託者資通安全維護情形應注意事項	2.111年本機關計　　份契約： 〇全部契約皆已納入前述規定。 〇其中　　份契約已納入前述規定，其餘未納入之原因為：_____ 〇全部契約皆未納入相關規定，原因為：_____ 補充說明(選填)：_____
	10.3是否辦理委外廠商查核?	(單選) 〇　本機關無資通系統或服務委外 〇　本機關111年委外資通系統、服務廠商共計_____家 111年**自行辦理**委外廠商查核，計查核____家，受查核廠商為_____，查核方式為_____(例如實地查核、書面查核等)；111年**聯合其他機關**(包含_____等機關)**辦理**委外廠商聯合查核，計查核____ __家委外廠商，受查核廠商為_____，查核方式為_____。 **註：如查核廠商多於一家，請用頓號區隔，例如：A公司、B公司** 〇　111年未進行委外廠商查核，原因為：_____ 補充說明(選填)：_____

實施情形檢查表10

實施項目	實施內容	辦理情形
11.資通安全教育訓練	11.1機關人員接受資通安全教育訓練情形	詳本機關應辦事項-資通安全教育訓練。
12.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	12.1訂定考核機制並進行考核	○111年資通安全考核獎懲情形：記獎 人、懲 人。 ○111年資通安全考核獎懲情形：無獎懲 ○111年無進行相關考核 補充說明(選填)：
13.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	13.1資通安全維護計畫實施情形之稽核機制	A~C級機關 ○本機關內部稽核機制已訂定於 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 文件(編號、名稱及章節)。本機關內部單位共有?個，內部稽核對象共有?個單位，稽核規劃為每年?個，預於 年內可完成全部單位稽核。(今年為第?年)。 稽核小組成員包含 個單位，共 人，每次稽核成員規劃為 (人數及組成規則)。 ○尚未訂定機關內部稽核計畫 D~E機關 ○本機關已訂定資安內部稽核機制。 ○本機關無資安內部稽核機制。 A~E級機關：補充說明(選填)：

實施情形檢查表11

實施項目	實施內容	辦理情形
13.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	13.2資通安全維護計畫之持續精進及績效管理	A~C級機關 〇本機關定期每?個月檢視及追蹤內部稽核改善執行情形。 〇本機關不定期檢視及追蹤內部稽核改善執行情形，方法為 〇未追蹤原因為： 補充說明(選填)： D、E級機關
	13.3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	1.無所屬/所監督公務機關 2.無所管特定非公務機關。
	13.4對所屬/所監督/所管機關(構)訂定稽核計畫	1.無所屬/所監督公務機關 2.無所管特定非公務機關
	13.5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	1.無所屬/所監督公務機關 2. (1)無所管CI提供者。 (2)無所管公營事業。 (3)無所管財團法人。

資通安全責任等級分級辦法

- 附表五 資通安全責任等級 C 級之公務機關應辦事項
- 附表七 資通安全責任等級 D 級之各機關應辦事項

C級單位應辦事項-管理面

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。(附表三)
	資訊安全管理系統之導入及通過公正第三方之驗證		C級必需導入ISMS。 教育體系資通安全暨個人資料管理規範
	資通安全專責人員		檢視並依附表1資安專職人力情形填報內容如下： 已完成：本機關之資安專職人員數量已達法遵要求 未完成：本機關之資安專職人員數量未達法遵要求，原因。說明: _____ 。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。

C級單位應辦事項-管理面

辦理項目及辦理細項	辦理內容	完成(Y/N)	符合進度(Y/N)	辦理現況
資通系統分級及防護基準	初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。	○Yes ○No	○Yes ○No	○ 已完成：本機關已針對自行(委外)開發之資通系統完成資通系統分級(詳如附表3-資通系統資產清冊)，並完成資通系統防護基準之控制措施。 ○ 未完成：本機關已針對自行(委外)開發之資通系統完成資通系統分級(詳如附表3-資通系統資產清冊)，但仍未完成資通系統防護基準之控制措施，預計於___年月前完成。 ○ 未完成：本機關未針對自行(委外)開發之資通系統完成資通系統分級(詳如附表3-資通系統資產清冊)及完成資通系統防護基準之控制措施，預計於___年___月前完成。 補充說明(選填)：
資訊安全管理系統之導入	初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。	○Yes ○No	○Yes ○No	○ 已完成：本機關已完成全部核心資通系統導入CNS 27001、ISO 27001或其他標準。 輔導廠商[註1]為：_____其它輔導廠商：_____（若為「其它」則需於本欄填寫廠商全稱） ○ 未完成：本機關尚未完成ISMS導入，預計於___年___月前完成 輔導廠商[註1]為：_____ 其它輔導廠商：_____（若為「其它」則需於本欄填寫廠商全稱） 補充說明(選填)： 註1：「輔導廠商」係依歷年各機關填報資料及共同供應契約廠商建置選項，若非屬上述廠商請將廠商全稱填寫於「其他輔導廠商」

C級單位應辦事項-管理面

辦理項目及辦理細項	辦理內容	完成(Y/N)	符合進度(Y/N)	辦理現況
資通安全專責人員	初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。	OYes ONo	OYes ONo	請檢視並依附表1資安專職人力情形填報內容如下： O 已完成：本機關之資安專職人員數量已達法遵要求 O 未完成：本機關之資安專職人員數量未達法遵要求，原因說明：_____。 補充說明(選填)：
內部資通安全稽核	每二年辦理一次。	OYes ONo	OYes ONo	O 已完成：已完成規定次數之內部稽核，計有_____項改善建議，預計(已)於_____年_____月前完成改善。 O 未完成：預計於___年___月前完成內部稽核。 O 未完成：未進行機關內部稽核，原因說明： 。 補充說明(選填)： **註：請依【資通安全維護計畫實施情形檢核表】13.1填寫內部稽核情形**
業務持續運作演練	全部核心資通系統每二年辦理一次。	OYes ONo	OYes ONo	O 已完成：已完成全部核心資通系統業務持續運作演練 O 未完成：已完成_____個核心資通系統業務持續運作演練，剩餘核心資通系統業務持續運作演練預計於_____年_____月完成。 補充說明(選填)： **註：如有非核心系統進行業務持續運作演練，請於補充說明欄位註明**

C級單位應辦事項-技術面

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	
	資通安全健診	網路架構檢視	每二年辦理一次
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	

C級單位應辦事項-技術面2

制度面向	辦理項目	辦理項目細項	辦理內容
	資通安全弱點通報機制(VANS)		一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

C級單位應辦事項-技術面

辦理項目及辦理細項	辦理內容	完成(Y/N)	符合進度(Y/N)	辦理現況
安全性檢測-弱點掃描	全部核心資通系統每二年辦理一次。	○Yes ○No	○Yes ○No	○ 已完成：本機關已完成全部核心資通系統規定次數之弱點掃描，共發現___項弱點，已(將)於___年___月完成修補。 弱點掃描廠商[註2]為：_____ 其它弱點掃描廠商：_____(若為「其它」則需於本欄填寫廠商全稱) ○ 未完成：本機關已完成___個核心資通系統規定次數之弱點掃描，共發現___項弱點，已(將)於___年___月完成修補，其餘核心資通系統規定次數之弱點掃描，預計將於___年___月前完成。 補充說明(選填)： **註2：「弱點掃描廠商」係依歷年各機關填報資料及共同供應契約廠商建置選項，若非屬上述廠商請將廠商全稱填寫於「其他弱點掃描廠商」**
安全性檢測-滲透測試	全部核心資通系統每二年辦理一次。	○Yes ○No	○Yes ○No	○ 已完成：已完成全部___個核心資通系統滲透測試 滲透測試廠商[註3]為：_____ 其它滲透測試廠商：_____(若為「其它」則需於本欄填寫廠商全稱) ○ 未完成：已完成___個核心資通系統滲透測試，其餘核心資通系統滲透測試，將於___年___月前完成。 補充說明(選填)： **註3：「滲透測試廠商」係依歷年各機關填報資料及共同供應契約廠商建置選項，若非屬上述廠商請將廠商全稱填寫於「其他滲透測試廠商」**

C級單位應辦事項-技術面

辦理項目及辦理細項	辦理內容	完成(Y/N)	符合進度(Y/N)	辦理現況
資通安全健診- 網路架構檢視	每二年辦理一次。	○Yes ○No	○Yes ○No	○ 已完成：本機關已辦理網路架構檢視(含檢視特權帳號管理者與一般使用者是否區分使用網段)，發現___項問題，已(將)於___年___月完成改善。 ○ 未完成：預計於___年___月完成檢視 補充說明(選填)：
資通安全健診- 網路惡意活動檢視		○Yes ○No	○Yes ○No	○ 已完成：本機關已辦理網路惡意活動檢視，發現___項問題，已(將)於___年___月完成改善。 ○ 未完成：預計於___年___月完成檢視 補充說明(選填)：
資通安全健診- 使用者端電腦惡意活動檢視		○Yes ○No	○Yes ○No	○ 已完成：本機關已辦理使用者端惡意活動檢視，機關內部電腦共___台，共執行台電腦發現___項問題，已(將)於___年___月完成改善。 ○ 未完成：預計於___年___月完成檢視 補充說明(選填)：
資通安全健診- 伺服器主機惡意活動檢視		○Yes ○No	○Yes ○No	○ 已完成：本機關已辦理伺服器主機惡意活動檢視，機關內部伺服器共___台，共執行___台伺服器發現___項問題，已(將)於___年___月完成改善。 ○ 未完成：預計於___年___月完成檢視 補充說明(選填)：
資通安全健診- 目錄伺服器設定及防火牆連線設定檢視		○Yes ○No	○Yes ○No	○ 已完成：本機關已辦理目錄伺服器設定及防火牆連線設定檢視，共發現___項問題，已(將)於___年 ___月完成改善。 ○ 未完成：預計於___年___月完成檢視 補充說明(選填)：

C級單位應辦事項-技術面

辦理項目及辦理細項	辦理內容	完成(Y/N)	符合進度(Y/N)	辦理現況
資通安全弱點通報機制	一、初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料	○Yes ○No	○Yes ○No	○ 已完成：本機關已完成資通安全弱點通報機制導入作業。 資通安全弱點通報機制廠商[註4]為：_____ 其它資通安全弱點通報機制廠商：_____（若為「其它」則需於本欄填寫廠商全稱) ○ 未完成：預計於_____年_____月前完成資通安全弱點通報機制導入作業。 補充說明(選填)： **註4：「資通安全弱點通報機制廠商」係依歷年各機關填報資料及共同供應契約廠商建置選項，若非屬上述廠商請將廠商全稱填寫於「其他資通安全弱點通報機制廠商」**
資通安全防護- 防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。	○Yes ○No	○Yes ○No	○ 已完成：本機關已完成防毒軟體之建置，將持續使用及適時進行軟、硬體之必要更新或升級 ○ 未完成：尚未完成防毒軟體之建置，原因為 補充說明(選填)：
資通安全防護- 網路防火牆		○Yes ○No	○Yes ○No	○ 已完成：本機關已完成網路防火牆之建置，將持續使用及適時進行軟、硬體之必要更新或升級。 ○ 未完成：尚未完成網路防火牆之建置，原因為 補充說明(選填)：
資通安全防護- 具有郵件伺服器者，應備電子郵件過濾機制		○Yes ○No ○不適用	○Yes ○No ○不適用	○ 已完成：本機關電子郵件伺服器已具備電子郵件過濾機制，將持續使用及適時進行軟硬體之必要更新或升級。 ○ 未完成：本機關具電子郵件伺服器，但尚未具備電子郵件過濾機制，原因為 ○ 不適用：本機關無電子郵件伺服器。 補充說明(選填)：

C級單位應辦事項-認知與訓練

制度面向	辦理項目	辦理項目細項	辦理內容
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		資通安全教育訓練	(A、B、C、D、E、公務、特定非公務皆同) 每人每年接受三小時以上之資通安全通識教育訓練。

C級單位應辦事項-認知與訓練

辦理項目及辦理細項	辦理內容	完成(Y/N)	符合進度(Y/N)	辦理現況
資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。	○Yes ○No	○Yes ○No	○ 已完成：本機關資通安全專職人員均已符合規定。 ○ 未完成：本機關資通安全專職人員其中＿＿＿人已符合規定，＿＿＿人未符規定， 改善措施：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿。 補充說明(選填)：
資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。	○Yes ○No	○Yes ○No	○ 已完成：本機關資通安全專職人員以外之資訊人員均已符合規定。 ○ 未完成：本機關資通安全專職人員以外之資訊人員共＿＿＿人，其中＿＿＿人已符合規定，＿＿＿人未符規定，改善措施： 。 補充說明(選填)：
一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。	○Yes ○No	○Yes ○No	○ 已完成：本機關一般使用者及主管均已符合規定。 ○ 未完成：本機關一般使用者及主管共＿＿＿人，其中＿＿＿人已符合規定，人未符規定， 改善措施：＿＿＿＿＿＿＿＿＿＿＿＿。 補充說明(選填)：

D級單位應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
認知與訓練	資通安全教育訓練	一般使用者及主管	(A、B、C、D、E、公務、特定非公務皆同) 每人每年接受三小時以上之資通安全通識教育訓練。

D級單位應辦事項-技術面及認知與教育訓練

辦理項目及辦理細項	辦理內容	完成(Y/N)	符合進度(Y/N)	辦理現況
資通安全防護- 防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級	○Yes ○No	○Yes ○No	○ 已完成：本機關已完成防毒軟體之建置，將持續使用及適時進行軟、硬體之必要更新或升級。 ○ 未完成：尚未完成防毒軟體之建置，原因為 補充說明(選填)：
資通安全防護- 網路防火牆		○Yes ○No	○Yes ○No	○ 已完成：本機關已完成網路防火牆之建置，將持續使用及適時進行軟、硬體之必要更新或升級。 ○ 未完成：尚未完成防毒軟體之建置，原因為 補充說明(選填)：
一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。	○Yes ○No	○Yes ○No	○ 已完成：本機關一般使用者及主管均已符合規定。 ○ 未完成：本機關一般使用者及主管共_____人，其中_____人已符合規定，人未符規定， 改善措施：_____。 補充說明(選填)：

感謝聆聽

聯絡方式：05-2787140#139　E-mail：liu0604@mail.edu.tw