國家發展委員會

花東基金補助計畫管理資訊系統建置

委外服務案

(案號：ndc112003)

需求說明書

中華民國　年　月

目次

[壹、專案說明 2](#_Toc120633327)

[一、專案名稱 2](#_Toc120633328)

[二、背景說明 2](#_Toc120633329)

[三、專案目標 3](#_Toc120633330)

[四、專案範圍 3](#_Toc120633331)

[五、專案時程 4](#_Toc120633332)

[六、專案預算 4](#_Toc120633333)

[貳、專案需求說明 5](#_Toc120633334)

[一、共通性規範 5](#_Toc120633335)

[二、花東基金補助計畫管理資訊系統建置 6](#_Toc120633336)

[三、跨系統資料介接 9](#_Toc120633337)

[四、駐點人員 9](#_Toc120633338)

[五、客服專線諮詢服務 9](#_Toc120633339)

[六、教育訓練 10](#_Toc120633340)

[參、資訊安全及保密責任要求 11](#_Toc120633341)

[肆、其他事項 13](#_Toc120633342)

[伍、基本服務水準 14](#_Toc120633343)

[陸、交付項目 17](#_Toc120633344)

[柒、服務建議書建議格式 18](#_Toc120633345)

[附件1：花東基金補助計畫管理資訊系統操作畫面範例 19](#_Toc120633346)

[附件2：花東基金補助計畫管理資訊系統資料欄位範例 20](#_Toc120633347)

[附件3：資通系統共同性基本安全要求 28](#_Toc120633348)

[附件4：變更申請單 66](#_Toc120633349)

[附件5：經費估算表 69](#_Toc120633350)

# 壹、專案說明

## 一、專案名稱

花東基金補助計畫管理資訊系統建置委外服務案（以下簡稱本專案）。

## 二、背景說明

**（一）專案緣起**

為推動花東地區產業發展，維護自然生態景觀，發展多元文化特色，提升生活環境品質，100年6月29日總統令公布「花東地區發展條例」(以下簡稱花東條例)，行政院同時依據花東條例第12條規定，設立「花東地區永續發展基金」(以下簡稱花東基金)，用以支應補助花東地區永續發展相關計畫，以及辦理花東產業輔導與投、融資計畫等。

花東兩縣政府依花東地區永續發展策略計畫，擬訂4年1期之綜合發展實施方案，迄今業推動至第3期，第4期綜合發展實施方案（表定為113年至116年）預定於112年啟動編擬及審議作業，為使各項基金補助計畫能如期於執行期間以更有效率及便捷方式管理，擬於本專案開發建置管理資訊系統，以強化花東地區永續發展基金補助計畫(以下簡稱花東基金補助計畫)執行管理。

本專案規劃在相關計畫體制及管考規定基礎上，配合最新資訊安全規範，建構符合中央主管部會及計畫執行機關計畫經費控管、執行管理、成果彙總等管理需求之管理系統，並且提供與本會目前已開發建置之「政府計畫資料庫」及「個案計畫空間管理資訊系統」資料介接功能，以協助花東基金補助計畫建構地理空間資訊，未來進一步推動計畫資料治理等工作，完善整體計畫管理體制。

**（二）使用對象**

1、中央主管部會：花東基金補助計畫之中央主管部會。

2、縣政府：花蓮縣政府及臺東縣政府各計畫執行單位及管考單位。

3、本會各計畫審議及管制單位。

**（三）系統使用及開發環境**

本專案以行政院及所屬委員會雲端資料中心現行所提供各類型虛擬主機之規格及作業系統環境為準，雲端提供系統平臺包含Windows及Linux，由得標廠商評估系統開發適合之版本，而資料庫軟體則需由得標廠商依開發方式自行採購授權及安裝設定。系統建置過程中如有其他環境需求，需由得標廠商依需求自行添購；後續視系統分階段建置情形由廠商增加相關軟硬體設備、伺服器或雲端空間服務。

## 三、專案目標

（一）提升花東基金補助計畫管考執行效能，建置花東基金補助計畫管理資訊系統。

（二）配合花東基金補助計畫主辦、管考及主管部會角色功能，提供使用者友善線上填審操作介面。

（三）建置整體計畫查詢及統計功能，輔以視覺化儀表版功能，提供整合性計畫管理資訊，並維護本系統功能正常運作。

（四）配合本會「政府計畫資料庫」(GDB) 之單一登入入口，以及「個案計畫空間管理資訊系統」(GISP)圖資點位填報正確資料。

（五）依資訊安全相關規範，確保本專案各伺服主機、應用程式之安全性。

## 四、專案範圍

本專案之範圍依專案目標分述如下（詳細內容請參閱貳、專案需求說明）：

（一）本案建置之花東基金補助計畫管理資訊系統，提供使用者友善之操作介面、搜尋功能及彈性報表，並依不同使用者有權限設定功能。

（二）將本會、中央主管部會及花蓮縣、臺東縣政府使用花東基金補助計畫管理資訊系統者之需求訪談，列入系統功能架構之參據。

（三）為提升系統穩定度以及降低系統客服頻率，應提供系統客服專線服務，並且辦理系統教育訓練。

（四）依據本階段需求訪談及系統建置等情形，提出後續系統功能增修及視覺化精進建議。

## 五、專案時程

本專案期程為自決標次日起至112年11月30日止。

## 六、專案預算

（一）本專案預算為新臺幣（以下同）400萬元整。如因112年度預算依法定程序全部或一部分未獲審議通過時，本會得終止契約或依立法院通過之預算額度調整工作項目內容，廠商得依「政府採購法」第64條規定辦理。

（二）機關得依政府採購法第22條第1項第7款規定，就廠商在本契約內所提供之各項服務，保留本契約後續擴充之權利，期限為履約完成日起2年內，上限金額新臺幣300萬元整，擴充項目包含持續辦理系統各項管理功能增修、設計多元化彈性報表、系統維運等。機關得視履約之工作執行及預算核定情形，於履約完成日前通知得標廠商提出下一期之工作計畫書，俟機關審查通過並簽奉核定後，由機關與得標廠商議價簽約。如得標廠商拒絕或未提送工作計畫書或審查不通過，由機關重新辦理招標。

（三）預計擴充項目說明如下(實際需求視本會日後提出之需求書為準)：

1、持續辦理花東基金補助計畫管理資訊系統各項管理功能增修。

2、設計多元化彈性報表，並依不同使用者需求產製視覺化報表及圖表，以因應資訊發展趨勢，提供資料加值應用服務。

3、本專案系統維運作業，包含應提供專業客服人員、辦理系統操作教育訓練、系統使用滿意度調查，辦理系統功能調整及增修、軟硬體資源及設備後續更新擴充、系統保固(含本專案開發系統保固期滿後之增購保固服務)等。

# 貳、專案需求說明

## 一、共通性規範

**（一）軟硬體需求**

1、本專案以使用「行政院及所屬委員會雲端資料中心」現行所提供各類型虛擬主機之規格及作業系統環境為準，所提供之基礎服務、資源運算服務（含虛擬主機、儲存空間、網路服務、負載平衡服務、自動擴展服務、備份服務等）、用戶自助服務管理、虛擬化資源動態調配及統合管理等服務為原則。雲端提供系統平臺包含Windows及Linux，由得標廠商評估系統開發適合之版本，而資料庫軟體則需由得標廠商依開發方式自行採購授權及安裝設定。系統建置過程中如有其他環境需求，需由得標廠商依需求自行添購；後續視系統分階段建置情形由廠商增加相關軟硬體設備、伺服器或雲端空間服務。

2、系統應支援橫向擴充(Scale-Out)能力，並具備無狀態(Stateless)特性，可支援分散式、平行式處理需求及彈性容量管理，以確保因應使用者大量的服務請求，可同時支援多個相同服務於不同主機運行，以支援自動擴展與負載平衡機制。

3、網站應以HTTPS安全通訊協議(SSL加密、認證機制)進行網頁開發，網頁錯誤訊息之顯示應經適當處理，不得直接顯示系統原始錯誤資訊(如SQL語法、系統版本等資訊)，以加強網路應用的安全性。

**（二）安全需求**

1、應參考行政院國家資通安全會報技術服務中心所發布之「Web應用程式安全參考指引」(請至nccst下載最新版)及「開放網路軟體安全計畫(Open Web Application Security Project ,OWASP) TOP 10最新版」之相關規範，減少Web 應用程式可能發生的攻擊弱點，並注意系統開發階段相關安全議題，以降低機關資安風險。

2、系統測試時或安裝前廠商進行安全性測試，倘發現資訊安全漏洞時，須主動進行修正作業，並確認作業系統及應用系統版本升級或修補程式時，須對其進行審查和測試，以確保應用系統的穩定性與安全性；如因系統限制無法升級或修補，應提出因應措施。

3、系統上線前，應提供資通系統之第三方安全性檢測證明，並完成高、中弱點修補作業(包含作業系統及應用系統等安全性更新)並填寫「ISMS-B.05-03 弱點處理報告表\_v3.0」(如附件3之附表6)，於完成修補後綜整提交「資訊安全檢測報告」。

4、日誌管理，系統應至少留存網站使用紀錄6個月以上，並定期備份於外部設備，至少包含作業系統日誌、網站日誌、應用系統日誌及登入日誌，紀錄內容應至少包含時間、來源IP、連結網址、機關別、使用者姓名、使用者身分(依系統使用權限區分)、功能名稱等欄位，本項紀錄應至少可匯出為excel、csv及odf等檔案格式，並納入月工作報告中；廠商應針對程式碼之版控維持一定量數(如：保留3代)。

5、廠商倘使用非自行開發之元件，應標示其來源並提出授權證明，並依程序填報「軟體清冊」。

**（三）功能測試**

1、廠商應就建置之系統功能擬定「測試計畫」，以測試所有軟體單元，確保系統運作正常及內外部介面之相容性，測試前應確保測試環境各端點安全，並避免使用正式區之資料或真實資料作為測試資料，系統測試計畫內容包括測試工具、測試需求、測試個案、測試程序、測試負責人及測試時程。

2、廠商須依據系統測試計畫會同本會人員執行系統測試作業，並記錄測試結果，若測試結果不正確，應修正並執行必要之迴歸測試，並記錄與保存所有測試過程與結果，綜整提交「測試報告」。

## 二、花東基金補助計畫管理資訊系統建置

得標廠商於本專案簽約後，須與本會、中央主管部會及花東兩縣政府相關單位承辦人員進行訪談，評估現行管理資訊系統使用情形，以確認各承辦角色對於重新建置系統之功能需求，完成建置系統之架構，並配合系統上線時程提供使用者操作手冊及系統操作影片，規劃如下：

（一）得標廠商依本專案系統使用者角色設定帳號權限，使用者各自皆有帳號密碼，系統畫面與提供的功能配合登入使用者層級及角色不同而有權限差異，所能閱覽之內容也有所不同，並須由本會政府計畫資料庫(GDB)單一入口登入，需配合與該會員中心進行整合，透過身分認證標準協議實作網站單一登入，導引使用者至會員中心進行帳號註冊、並完成系統使用者與會員中心帳號間之綁定機制。本專案系統另應提供系統使用者及管理者角色依帳號管理機制，執行帳號申請、建立、修改、啟用、停用及刪除等程序之功能，使用者權限架構如下：

1、本會管制考核處：計畫資料上傳及下載、所有報表查詢使用功能、異常填報或落後案件之提醒報表及考核相關功能等。

2、本會國土區域離島發展處：計畫資料上傳及下載、基金撥款及繳回數資料維護、所有報表查詢使用功能。

3、中央主管部會：主管計畫資料上傳及下載、績效檢討作業資料匯出、報表查詢使用功能。

4、縣政府管考：計畫資料新增及登錄、計畫資料上傳及下載、報表查詢使用功能、計畫資料填報、修改或落後案件之提醒功能及報表等。

5、縣政府案件主辦：業管計畫資料新增及登錄、計畫執行情形填報或落後案件之提醒功能等。

（二）得標廠商應依本會需求提供相關客製報表及彈性報表，並配合本會管考需求協助產製相關報表。

（三）其他基本功能如下：

1、**資料填報歷程紀錄及鎖定功能：**資料填報應紀錄每次填報和修正的時間及人名，於系統顯示歷程紀錄，並於各項資料填報時間截止後將資料鎖定，避免任意修改。

2、**資料備份功能：**系統資料於填報週期截止後，應留存當期資料版本，以作為後續資料查對之基礎。

3、**落後案件自動提醒或稽催功能：**針對應填報未填報項目，應建立自動提醒或稽催功能，如未於填報時間內完成即自動通知負責填報人及管考人員。

4、**本會雲端機房應建立測試機：**不同系統介接時需測試以符合資安要求；未來建議精進資料保存技術及加值運用功能，保存空間也需納入評估。

5、**跨年度報表或跨年度計畫之間的關聯分析功能：**呈現跨年度之間關聯分析功能。

（四）得標廠商對於國發會、中央部會及花東兩縣使用者以座談會方式辦理需求訪談，分別於臺北市辦理2場、花蓮縣及臺東縣各辦理1場次座談會，各場次邀約對象需由本會決定，每次訪談結果應做成紀錄。

1、系統應提供使用者容易檢視之版面、簡化操作介面及作業流程，並依使用者角色需求設定不同功能。

2、計畫資料應不限於整批上傳，亦可自行新增、登錄及填報，並依使用者需求完成系統各類報表功能。

（五）建置預估時程如下表，請搭配「陸、交付項目」

| 辦理期程 | 工作內容 |
| --- | --- |
| 112年3月15日前 | 1.辦理4場需求訪談2.帳號權限控管3.系統規劃報告 |
| 112年6月30日前 | 1.架設測試機及測試系統功能2.與其他系統介接規劃3.系統上線規劃書4.教育訓練規劃書 |
| 112年9月30日前 | 1.系統教育訓練3場2.系統客服服務3.完成與本會其他系統介接(GDB及GISP) |
| 112年10月5日前 | 1.系統後續擴充功能建議2.系統正式上線使用 |

## 三、跨系統資料介接

 確保「花東基金補助計畫管理資訊系統」(本專案系統)與本會其他系統之資料整合，建立跨系統資料介接，本專案系統應與本會「政府計畫資料庫」(GDB)及「個案計畫空間管理資訊系統」(GISP)介接。

（一）本專案花東基金補助計畫管理資訊系統須配合介接本會「政府計畫資料庫」(GDB)系統，由GDB單一入口登入，登入後點選連結至本專案系統，得標廠商須依使用者角色設定該帳號於系統之權限。配合本會政府計畫資料庫(GDB)辦理單一登入機制與會員中心建置需求，相關工作說明如下：

1. 提供會員中心登入後，花東系統的預設頁面網址、依指定格式提供系統會員資料，以及依指定格式和指定權限驗證的會員狀態API等相關資訊。

2. 於花東系統登入頁放置「會員中心」代登入連結、將花東系統既有註冊頁導引至「會員中心」註冊頁，以及單一登入機制驗測等事宜。

（二）本專案花東基金補助計畫管理資訊系統計畫空間資料，須至本會「個案計畫空間管理資訊系統」(GISP)系統填報，相關介接作業之配合事項，包含提供GISP填報所需介接資料表的DB Schema文件與介接方式、系統串接服務資訊與防火牆規則等作業內容；上述內容需於本專案系統正式上線前3個月提供予GISP系統委外廠商。

## 四、駐點人員

本專案廠商應自決標次日起20日內指派1名具資訊及專案管理專長之駐點服務人力至112年11月30日止，辦理本案工作項目，並於決標次日後10日內檢送相關履歷至本會，派駐人員須大學以上畢業，熟悉GIS及資料庫軟體、具備3年以上資料處理相關工作經驗，專職襄理資訊業務及花東基金補助計畫資料管理。

## 五、客服專線諮詢服務

配合花東基金補助計畫管理資訊系統建置及上線情形，為協助系統使用及操作問題，應有2線客服專線服務：

（一）客服專線服務範圍為本專案資訊系統功能。

（二）配合公務機關上下班時間（不含公務機關例假日），每日自8時起至18時止；惟如發生主機停機、系統作業高峰期間、緊急或資安事件時，仍應彈性配合本會非上班時間之實際作業需求，進行必要之客服或技術人員調度增派。

（三）為維持系統正常運作，應提供使用者客服專線服務，內容包含操作諮詢服務、客戶申訴、異常主動通知及問題叫修處理服務等，各項諮詢專線服務內容應作成紀錄留存，作為系統調整及精進之參考，並適時後送系統工程人員，進行程式研判及修正，完成修正後應由客服人員回復使用者系統問題改善情形。

（四）每月系統客服諮詢服務應留存紀錄，客服紀錄內容應包含提問時間、提問管道(電話或電子郵件等)、提問單位、諮詢問題與處理方式以及完成時間等，固定於每月5日前(含5日)以電子郵件方式提交本會承辦人員，並呈現於各期報告書及結案報告書中。

（五）綜整前述問題彙整成系統常見問答集（FAQ），並每季檢視常見問答集、系統操作手冊及系統教育訓練講義等內容，必要時應於系統公布更新內容。

## 六、教育訓練

 配合花東基金補助計畫管理資訊系統建置及上線情形，為協助中央主管部會及花東兩縣政府承辦人員瞭解及熟悉系統之功能及操作，得標廠商應辦理3場次教育訓練(預計規劃臺北市、花蓮縣及臺東縣各1場次)：

（一）訓練課程時間、地點、場次，授課人員及其資格皆應先經本同意。

（二）每場次授課時數以3小時為原則，每場次教育訓練人數約為20 至40人，得標廠商提供每場次受訓學員所需教材(得以電子檔提供)及辦理報名聯繫等相關事宜。

（三）教育訓練成果報告至少包含課程資料(主題、日期及地點)、課程講義(得以電子檔提供)、上課人員簽到表、佐證相片及課程意見問卷調查結果等內容。

（四）外聘講師鐘點費、交通費、食宿費、教材編印費(如以電子檔提供則無須編列)、學員餐飲及訓練場地租用等費用由得標廠商支應，其中訓練場地得由本會協助洽借。

# 參、資訊安全及保密責任要求

一、資安架構及弱點掃瞄：相關系統資安設計，需配合本會資安架構加以修改，並依本會定期對各主機進行弱點掃描及滲透測試之結果，廠商須於1個月內完成中、高風險修補、2個月內完成低風險修補，並紀錄於弱點處理報告表。

二、應用系統資料存取管制機制：資料安全須包含使用權限管制存取管制，識別使用者身分，以防止非合法授權人進入等。

三、得標廠商須配合本會資訊安全管理機制進行內部抽查、稽核及外部稽核等作業，如有不符合處，須配合於期限內予以改善，並提供本案災害復原計畫，進行業務持續運作演練每年至少1次，機制與緊急通報程序。

四、主動完成本案相關主機防護（如防毒軟體病毒碼檢查與更新等）、作業系統、政府組態基準（GCB）、應用相關軟體等安全性更新作業，並視需要，出席資訊安全相關會議。

五、依據本專案系統評定之資訊系統等級為普級，得標廠商應遵守本會資通系統共同性基本安全要求(如附件3)完成相關資通安全防護控制措施。

六、系統更新前廠商應填寫變更申請單(如附件4)(包含:停機維護、作業系統升級、資料庫升級、版本更新等)，評估更新作業對系統之影響，或於測試環境測試無誤後再行申請更新作業，並視需要進行備份作業，如更新作業異動資產清冊內之項目，應更新資產清冊。

七、得標廠商必須遵循行政院資通安全管理法與本會現行資訊安全管理作業要求(如ISO/IEC27001、ISO/IEC27000)，以執行相關工作。

八、得標廠商對於系統之資源使用狀況及容量之需求，須設定容量管理值及執行監控，並交付於各期資安相關表單中，提供容量監控必要資訊(如：CPU\RAM使用率、硬碟容量或網路流量等)，倘達到設定值時，須通知本會承辦人並提供規劃建議。

九、依據本會資安管理制度規定，為強化廠商維護作業之安全性，廠商必須至本會始能連接系統，以執行更新及維運等工作。

十、本專案期間內，系統如遇資安攻擊事件，得標廠商應辦理第三方檢測並提供報告結果，以確保資訊系統安全。

十一、其他保密條款如下：

(一)得標廠商及人員對業務上所接觸之資料，應視同機密文件採必要之保密措施，並遵守本會資訊安全相關規定，本專案相關人員須簽寫「保密切結書」與「保密同意書」(依本會提供之格式)，上述文件應納入契約書。

(二)得標廠商及人員應接受適當的資通安全暨個資保護訓練，並提供相關佐證紀錄(如相關證照或受訓紀錄等)以確保人員瞭解機敏資料保護責任及適切使用設備與設施。

(三)得標廠商對於交付或告知之文件或資料，應負完全保密責任。

(四)得標廠商對所有資料均負永久保密責任，本專案因期限屆滿、解除或其他原因而終止後，得標廠商及其工作人員仍負有保密責任。

(五)對於本專案各項作業之執行，應採取權限管制措施，並依實際權限授與相對之執行功能及資料存取權限，確保相關資料安全防護。

(六)本會如發現保密標的遭受未授權之使用或有洩密之虞時，應立即通知得標廠商，並要求得標廠商採取必要防止措施。

(七)任何因得標廠商人員洩密所致之賠償或刑事責任，概由得標廠商負責，本會並得將其列入拒絕往來戶。

(八)契約終止時，得標廠商應將本會所提供之資料退還或銷毀，並應遵守「個人資料保護法」等相關規定。

十二、本會於本專案期程內，得就本節「資訊安全及保密責任要求」相關事項，對得標廠商應承擔之責任行使稽核權，並得至得標廠商之辦公處所執行必要之查核，得標廠商應配合提供相關資料及文件，得標廠商若有造假之情事，應負完全之法律責任。

# 肆、其他事項

一、指定專案負責人至少1人，負責本案整體作業規劃、人力配置、任務分派、進度控管、作業協調等專案管理相關工作，並配合本會舉行相關會議，說明各項辦理進度及執行情形。本案各項辦理情形，均須與本會密切聯繫，以確保專案內容確實執行。

二、本專案得標廠商應於議價完成後，依議價（包含價格以外事項）結果，提出本專案之「專案工作計畫書」，執行過程中如經雙方同意調整工作內容，應即時為必要之修正，不得拒絕。

三、本專案報告資料除書面外，應提供可供本會運用之電子檔格式資料（如\*.odf、\*.doc、\*.pdf、\*.ppt等）。

四、配合本會資訊推動政策，本專案相關功能匯出之資料格式應包含ODF等開放資料格式。

五、因應本會業務需求、環境或資訊安全驗證範圍變動，本專案各項服務、作業標的及驗證範圍亦配合調整時，相關成本費用未超過本案總價金5%，本會不另外給付費用。

六、配合本會需要擬定災害復原計畫，並完成1次災害復原演練作業。

七、系統安裝完成，由本會相關負責人員會同進行功能測試，功能測試正常後，再行辦理驗收事宜。

八、本專案自建置完成驗收之日起，廠商須提供1年保固與維運服務，包含本專案系統功能之除錯與效能調校、安全上微調修改。

九、本專案開發之系統、報表財產等之著作權及智慧財產權悉歸本會所有，且非經本會書面同意，本專案得標廠商不得為任何形式之複製或發表。

十、智慧財產權：

(一)簽約廠商交付之本案相關報告或文件如包含第三者開發之產品（或無法判斷是否為第三者之產品時），應保證其使用之合法性或提供授權證明文件（以符合中華民國著作權法規範為準），如隱瞞事實或取用未經合法授權之識別標誌、圖表及圖檔等，致使本會遭致任何損失或聲譽損害時，簽約廠商應負一切損害賠償責任（含訴訟及律師費用），並盡最大努力於訴訟或仲裁中為本會之權益辯護。

(二)本案簽約廠商應遵守著作權及專利法之相關規定，如有違反情事發生，簽約廠商應負完全之法律責任，與本會無關。

十一、本專案執行費用之撥付方式為本專案得標廠商先依契約規定以發票檢據核銷。

十二、本文件於決標後納入為契約之一部分。

十三、其他未盡事宜，依據「政府採購法」及其相關規定辦理。

# 伍、基本服務水準

一、本項服務水準係評估廠商對本專案之服務是否達到基本要求，如廠商未達服務水準要求時，本會得依下列服務水準協定(如表1)處懲罰性違約金。

二、服務水準協定（Service Level Agreement, SLA），本案各項服務水準協定（SLA），如廠商無法完成相關作業項目規定，其罰款計算方式為（累計罰則點數）X (總價金1‰) 元，同一評估項目具有2種（含）以上之評斷方式者，如廠商同時違反2種（含）以上時，其違約金係採罰責較重者。本案各項服務水準如有無法達成之情事，除經本會認定屬硬體設備所致外，得標廠商應負責完成符合服務水準之服務。

表1各評估項目服務水準

| 評估項目 | 服務水準指標 | 計算方式 | 處罰規則 |
| --- | --- | --- | --- |
| 文件及系統交付時程 | 依合約規定時程交付各項相關系統開發功能及文件 | A – B < 1日A：各項系統功能及文件預定交付日期B：各項系統功能及文件實際交付日期 | 每逾1日計罰1點，交付時程以前述建置期程、各期交付項目及時間表為準。 |
| 出席會議情形 | 得標廠商應配合本專案需求指派人員出席相關會議 | 未指派或未出席與本專案相關會議 | 按每人每次計罰1點。 |
| 故障排除、系統修復 | 系統發生故障，經機關通知（不限形式）後，4小時內修復或提供相同系統供機關暫時使用；並於2個工作天內完成並恢復正常運作 | A-B < 4小時A:回應本會並修復或提供機關暫時使用時間；恢復正常運作時間B:接獲本會通知時間 | 每逾2小時計罰1點；恢復正常運作時間每逾1個工作天計罰2點。 |
| 系統可用率 | 系統各項功能，累計中斷服務時間每季不得超過6小時 | 每季統計 | 每逾2小時計罰1點。 |
| 單日累計故障時數（不滿1小時，以1小時計） | 每日不得超過4小時 | 單日超過4小時每逾1小時計罰1點。 |
| 系統或功能測試及上線前後，經機關通知修正（不限形式）後，3個工作天內完成調整 | A-B < 3個工作天A:系統完成調整時間B:接獲本會通知時間 | 每逾1日計罰1點。 |
| 資安指標 | 未完成本資通系統防護基準控制措施項目 | 每次統計 | 每次不得超過1項，每逾1項計罰1點。 |
| 資通系統網站安全弱點檢測結果與滲透測試結果，屬於中、高風險項目需於1個月內修補完畢，低風險項目需於2個月內修補完畢 | 每次統計 | 每次不得超過1天，每逾1天計罰1點。 |
| 安全性檢測報告(資通系統分級屬於普級或中級繳交弱點掃描報告；資通系統分級屬於核心或高級繳交源碼掃描、弱點掃描及滲透測試報告) | 每次統計 | 每次不得超過1天，每逾1天計罰1點。 |
| 主機與系統弱點修補（如Windows Update） | 每季統計 | 每季不得超過1次，每逾1次計罰1點。 |
| 知悉發生資安事件應於1小時內通知機關（或接獲機關通知1小時內），並採取適當之應變措施**（資通安全事件通報單）** | A-B < 1小時A:廠商以電話、簡訊或mail回報處理情況之時間B:知悉發生資安事件或接獲機關通知處理資安事件之時間 | 每逾1小時計罰1點，每1資安事件可歸責於廠商者計罰1點。 |
| 完成損害控制或復原作業，得標廠商應於知悉資安事件後72小時(重大資安事件為36小時)內完成損害控制或復原作業 | 每次統計 | 每逾1小時計罰1點。 |
| 如發生資安事件，於完成損害控制或復原作業後，得標廠商應於1個月內送交調查、處理及改善報告 | 每次統計 | 每次不得超過1天，每逾1天計罰1點。 |
| 得標廠商於本專案範圍內，因未採取適當防護致機關敏感資料外洩或遭竄改 | 按受影響資料筆數 | 每10筆計1點。 |
| 廠商於本專案承接範圍內，因未採取適當防護，致機關個人資料外洩或遭竄改 | 按受影響資料筆數 | 每10筆計1點。 |

# 陸、交付項目

各期主要交付項目(如表2)，得標廠商應就完成本專案目標所需之交付項目提出整體規劃構想，並納入專案工作計畫書中：

一、各期交付內容及為完成本專案目標所需之交付文件，於工作計畫書中臚列整體細部項目及時程規劃。

二、各項交付項目文件均為一式2份，須以正式書面送交本會。所有交付項目文件均以A4尺寸紙張雙面列印製作及裝訂成冊，並皆須交付可攜式裝置一式2份，以供本專案查核與驗收付款依據。

表2 各期交付項目及時間表

| 期別 | 交付項目 | 交付時間 |
| --- | --- | --- |
| 第1期 | (一)專案工作計畫書（內容包含專案簡介、專案組織、人員分工職掌、專案管理機制、資通安全管理措施及各工作項目細部時程規劃）(二)花東基金補助計畫管理資訊系統雛形建置分析報告(含UI及權限控管)(三)完成4場需求訪談以及需求訪談紀錄 | (一)決標次日起20日內(二)、(三)於112年3月15日前 |
| 第2期 | (一)花東基金補助計畫管理資訊系統上線規劃書(二)花東基金補助計畫管理資訊系統測試報告(三)與本會其他系統介接規劃(四)資通系統共同性基本安全要求完工報告(含該要求之附件) 及日誌管理紀錄 | 112年6月30日前 |
| 第3期 | (一)結案報告（內容包含專案簡介、歷次需求訪談紀錄、系統各功能建置及測試報告、系統功能上線情形、系統操作手冊、與其他系統介接情形、客服服務工作報告及教育訓練成果報告等）(二)資訊安全執行情形及日誌管理紀錄(三)本專案系統開發建置之相關軟硬體資源(含軟體使用授權文件、完整系統原始程式碼及執行檔等) | 112年11月30日前 |

# 柒、服務建議書建議格式

（一）以中文由左至右（直式橫書）繕打，以14號字為原則，如有圖表得採用A3紙張，裝訂時應摺疊成A4尺寸，並加編封面、目錄及頁碼，A4紙張雙面列印一式10份。

（二）製作內容至少包括下列各項(請依機關提供之服務建議書內容所述撰寫，可自行調整目次及名稱或增加項目，應按評選項目製作頁次對照表)，各章節標題如下：

|  |
| --- |
| 壹、專案概述貳、執行能力及履約能力（內容包含廠商規模、背景及承製相關專案之實績、公司相關資訊安全政策、資安證明文件、獎項、人力資源應含資安人力等）參、技術建議肆、專案工作規劃與管理(內容包含資安作業，如履約程序及環境之資安管理規劃及執行方式，履約相關之資安事件通報、應變、處理之規劃機制，資安作業自評情形)伍、價格之完整性與合理性（需詳列報價內容，請依照附件5、經費估算表填列）陸、廠商企業社會責任(CSR)指標柒、其他說明事項及附件資料(各項附件、人員資歷、成果樣式、佐證資料及其他相關說明資料等) |

# 附件1：花東基金補助計畫管理資訊系統操作畫面範例





# 附件2：花東基金補助計畫管理資訊系統資料欄位範例

**（以下報表資料為示意，實際格式請依需求訪談確認之欄位及管理需求確認後訂之）**

**一、計畫基本資料**

**計畫基本資料表**

|  |  |  |  |
| --- | --- | --- | --- |
| 計畫名稱 |  | 計畫編號 |  |
| 計畫類別 |  | 計畫期程 |  |
| 中央主管機關 |  | 計畫核定總經費(千元) |  |
| 經費來源(花東基金) |  | 經費來源(中央預算) |  |
| 經費來源(地方預算) |  | 經費來源(其他) |  |
| 主辦縣府 |  | 縣府主辦單位 |  |
| 聯絡人員 |  | 職稱 |  |
| 電話 |  | 電子信箱 |  |
| 執行地點 |  |
| 計畫總目標 |  |
| 計畫預期效益 |  |
| 主要績效指標 |  |
| 計畫核定情形 | （上傳核定之行動計畫、全期工作計畫書） |

**\*經費來源(花東基金、中央預算、地方預算、其他)合計總金額應等於計畫核定總經費**

**二、年度作業計畫**

**壹、計畫概要**

**一、計畫基本資料**

|  |  |  |  |
| --- | --- | --- | --- |
| 計畫名稱 |  | 計畫編號 |  |
| 計畫期程 |  | 以前年度基金保留數 (千元)(I) |  |
| 計畫類別 |  |  基金當年核定數(千元)(J) |  |
| 中央主管機關 |  | 縣府主辦單位 |  |
| 主辦縣府 |  | 執行地點 |  |
| 計畫總目標 |  |
| 計畫年度目標 |  |
| 計畫核定情形 |  |

**計畫聯絡人資訊**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名 | 職稱 | 電話 | 傳真 | 電子郵件 |
|  |  |  |  |  |

**二、各年進度及預算配置**

|  |  |  |
| --- | --- | --- |
| 年度 | 工作摘要 | （花東基金）截至該年度數據 |
| 總累計進度(%) | 總累計分配經費(千元) | 總累計實現數(千元) |
| 預定 | 實際 |
| 112 |  |  |  |  |  |
| 113 |  |  |  |  |  |
| 114 |  |  |  |  |  |
| 115 |  |  |  |  |  |
| 備註 |  |

**貳、預算配置－各年預算編列使用**

**單位：新臺幣千元**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 年度 | 花東基金 | 中央預算 | 地方預算 | 其他 | 合計 | 預算使用 |
| 年編預算 | 以前年度保留 | 年度納管數 | 年編預算 | 以前年度保留 | 年編預算 | 以前年度保留 | 年編預算 | 以前年度保留 |  | 實現數 | 保留數 | 未保留數(繳回數) |
| 112 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 113 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 114 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 115 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 備註 |  |

**參、工作項目（以下資料以花東基金款填寫）**

|  |  |  |  |
| --- | --- | --- | --- |
| 序號 | 工作項目（本表由以下填報資料自動帶出） | 基金年度納管數 | 經費占比（％） |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 小計 |  |  |  |

**一、工作項目名稱：OOOOOOO（依工作項目項數往下衍生）**

**(一) 分月進度、預算配置及查核點**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 月份 | 工作摘要 | 查核點 | 年累計預定進度(%) | 年累計分配經費(千元) |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  | ● OOOO ( 預定 109/08/15 完成 ) |  |  |
| 9 |  | ● OOOO ( 預定 109/09/01 開始) |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |

**(二) 年度目標**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 項次 | 類別 | 工作內容 | 單位 | 截至上年度總累計目標執行數 | 當年度目標 | 總目標 |
|  |  |  |  |  |  |  |

**肆、整體計畫進度及預算配置（以上各工作項目加總）**

|  |  |  |
| --- | --- | --- |
| 月份 | 預定進度(%) | 分配經費(千元) |
| 總累計 | 年累計 | 總累計 | 年累計 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |

**三、計畫執行情形**

**112年O月執行進度**

**壹、計畫資訊**

**一、基本資料**

|  |  |  |  |
| --- | --- | --- | --- |
| 計畫名稱 |  | 計畫編號 |  |
| 計畫期程 |  | 以前年度基金保留數 (千元)(I) |  |
| 計畫類別 |  |  基金當年核定數(千元)(J) |  |
| 中央主管機關 |  | 基金全年納管數(千元)(K) |  |
| 主辦縣府 |  | 縣府主辦單位 |  |
| 執行地點 |  | 空間資料 |  |
| 計畫核定情形 |  |
| 計畫年度目標 |  |
| 計畫年度摘要 |  |

　**二、聯絡人員**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 職稱 | 姓名 | 聯絡電話 | 傳真 | 電子信箱 | 負責工作項目 |
|  |  |  |  |  |  |

**貳、整體計畫執行情形（執行數以基金款計算）**

**一、計畫進度與經費達成率**

**(一)當年度各月基金執行率**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 月 | 當月執行進度 | 基金累計至當月執行數 | 基金擬保留數 | 基金累計至當月分配數 | 年分配基金執行率 |
| 基金當月分配數(實際進度) | 花東基金實現數(元) | 基金累計實現數 | 基金已執行應付未付數 | 基金預付數 | 基金節餘數 | 小計 |
| 1 |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |
| 總計 |  |  |  |  |  |  |  |  |  |  |

**(二)累計至當月基金經費執行率**

|  |  |  |  |
| --- | --- | --- | --- |
| 計畫進度 | 預定進度(A)(%) | 實際進度(B)(%) | 進度比較(B-A)百分點 |
| 年累計 |  |  |  |
| 總累計 |  |  |  |
| 經費使用(千元) | 分配數(C) | 實現數(D) | 支用比(%)(D/C) | 已執行應付未付數(E) | 節餘數(F) | 預付數(G) | 執行數(H = D+E+F+G) | 分配經費執行率(%) (H/C) |
| 年累計 |  |  |  |  |  |  |  |  |
| 總累計 |  |  |  |  |  |  |  |  |
| 經費達成率(%) | 年計畫經費達成率(H)/(K) |  |
| 總計畫經費達成率(H)/(J) |  |
| 計畫核定經費達成率(H)/(I) |  |

**二、目標達成分析**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 項次 | 工作內容類別 | 工作內容 | 單位 | 截至上年度總累計目標執行數 | 年度目標(預定) | 年度目標(實際) | 總目標值(預定) |
|  |  |  |  |  |  |  |  |

**三、落後原因分析（請將下表落後原因及改善對策帶入）**

|  |
| --- |
| **總累計進度落後幅度大於 1 個百分點，年累計進度落後幅度大於 5 個百分點，年累計支用比未達 90%，年分配經費執行率未達 90%者必填** |
| 落後原因 |  |
| 因應對策 |  |
| 縣府管考建議 |  |

**參、工作項目全年辦理情形**

**一、OOOOOOO（依工作項目項數往下衍生）**

**(一)辦理情形及落後改善對策**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 月份 | 預定工作摘要 | 辦理情形 | 落後原因 | 改善對策 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |

**(二)辦理情形及落後改善對策**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 月份 | 查核點名稱 | 預定完成日期 | 實際完成日期 | 辦理情形 |
| 1 |  | 112/03/31完成 |  |  |
| 2 |  | 112/06/30完成 |  |  |
| 3 |  | 112/09/30完成 |  |  |
| 4 |  | 112/12/31完成 |  |  |

**肆、會計月報資訊**

|  |  |  |  |
| --- | --- | --- | --- |
| 月 | 基金待繼續支用數（會計月報） | 基金累計分配數（會計月報） | 基金累計實支數（會計月報） |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |

**伍、執行績效**

**(一)年度指標達成情形**

|  |  |  |  |
| --- | --- | --- | --- |
| 序號 | 年度指標 | 目標值 | 達成率 |
| 1 | 新增工作機會(+)(單位：人) | 13人 |  |
| 2 | 增加領養率(+)(單位：%) | 70 |  |
| 3 | 增加收容所節紮率(+)(單位：%) | 60 |  |
| 4 | 增加參訪人數(單位：人次/月) | 143 |  |

**(二)截至當月執行成果**

|  |
| --- |
| 執行效益說明 |
| 花蓮縣公立動物收容所遷建，主體建築至109年底已完成98.75%，增加30個以上工作機會。 |

# 附件3：資通系統共同性基本安全要求

**壹、資通系統應辦事項**

資通系統依據本會資訊安全管理制度之「風險評鑑管理要點」執行資通系統安全等級評估作業，鑑別本案資通系統防護需求等級如下：

▓普級

□中級

□高級

承商應依資通安全管理法及相關子法規定採行適當安全控制措施，以確保資通系統達到應具備之安全防護水準，並依下表，於專案起始1個月內辦理1次自評作業，之後則隨專案付款期程交付相關文件。

專案類型定義:

型一：專案採購金額達新臺幣1,000萬元以上。

**型二：專案採購金額未達新臺幣1,000萬元。**

型三：採購軟體即服務（Software as a Service,SaaS）或委外承商因執行專案所提供之套裝軟體工具或應用系統。

|  |  |  |
| --- | --- | --- |
| 應辦事項 | 專案類型 | 辦理情形說明 |
| 一 | **二** | 三 |
| 一、法規面要求 |
| 1. 依據「資通安全管理法施行細則」承商辦理本會業務得否分包、得分包之範圍與對象，及分包之合作承商應具備資通安全維護措施。
 | ○ | **○** | ○ | 本案不得分包 |
| 1. 依據本案資通系統資安等級於專案工作計畫書中說明資安控制項目，並完成「資通系統防護基準自評表」。
 | ○ | **○** |  | 填寫本會「資通系統防護基準自評表」 |
| 1. 本案如涉及國家機密者，執行本案承商之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。
 | ○ | **○** | ○ |  |
| 1. 依據行政院「資通安全管理法施行細則」該資通系統屬本會之核心資通系統，或委託金額達新臺幣一千萬元以上者，承商應另行委託第三方進行安全性檢測。
 | ○ |  |  |  |
| 1. 依據行政院「資通安全管理法施行細則」涉及利用非承商自行開發之系統或資源者，應標示非自行開發之內容與其來源及提供授權證明。
 | ○ | **○** | ○ | 型一和型二：填寫「系統套件清單」型三：出具使用授權證明。 |
| 1. 依據行政院「資通安全管理法施行細則」承商應提供資通系統之安全性檢測證明。(資通系統分級屬於普級或中級繳交弱點掃描報告；資通系統分級屬於核心或高級繳交源碼掃描、弱點掃描及滲透測試報告)
 | ○ | **○** | ○ |  |
| 1. 本會定期或於知悉承商發生可能影響本案之資通安全事件時，以稽核或其他適當方式確認本案之執行情形。
 | ○ | **○** | ○ |  |
| 1. 依據「資通安全管理法施行細則」，專案結束後承商來函說明本會相關專案資料返還、移交、刪除或銷毀狀況。
 | ○ | **○** | ○ |  |
| 1. 本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。
 | ○ | **○** | ○ |  |
| 1. 依據本會「共通性應用程式介面規範」開發符合OAS標準之API程式。
 | ○ | **○** |  |  |
| 1. 依據本會「網站無障礙規範」開發網站。
 | ○ | **○** |  |  |
| 1. 依據經濟部工業局「行動應用APP安全開發指引」和本會「[行動版應用程式(APP)無障礙開發指引](https://accessibility.ncc.gov.tw/Download/Detail/1425?Category=51)」開發行動APP。
 | ○ | **○** |  |  |
| 1. 依據經濟部工業局行動應用APP基本資安檢測基準」，委託第三方機構針對行動應用程式，進行資訊安全檢測。
 | ○ | **○** |  |  |
| 1. 依據行政院「各機關資通安全事件通報及應變處理作業程序」系統日誌(log)紀錄至少保留6個月，並定期備份於外部設備，應包含作業系統日誌(OS event log)、網站日誌(web log)、應用程式日誌(AP log)及登入日誌(logon log)。
 | ○ | **○** | ○ | 型一和型二：填寫「備份政策管理表」型三：出具日誌保留紀錄 |
| 1. 依行政院國家資通安全會報技術服務中心公告之項目，完成政府組態基準導入作業(<https://www.nccst.nat.gov.tw/GCB>)。
 | ○ | **○** |  | 於左列網址下載GCB說明文件，完成設定填寫於該文件備註欄，如有例外須填寫「GCB例外管理清單」 |
| 1. 依據「個人資料保護法」，如資訊設備與系統之紀錄倘含有個人資料檔案存取相關紀錄應至少保留5年以上，若無法線上保存，則應將紀錄匯出存檔備查。
 | ○ | **○** | ○ |  |
| 二、人力資源安全管理 |
| 1. 承商辦理本案之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
 | ○ | **○** | ○ | 於專案工作計畫書敘明 |
| 1. 承商應提供專案成員之資訊與資安專業能力證明文件 (數量、資格、證照、經驗)
 | ○ | **○** | ○ |  |
| 1. 承商於契約終止後，應歸還屬於本會之資產(包含：硬體、軟體、資料和系統存取權限等)，保密責任持續有效。
 | ○ | **○** | ○ |  |
| 三、資通系統環境與作業安全管理 |
| 1. 承商應配合本會盤點資訊資產。
 | ○ | **○** |  | 填寫「資訊資產清冊」 |
| 1. 開發、測試及線上運作之環境應設置於不同的網路區段或資訊處理設施。
 | ○ | **○** |  |  |
| 1. 作業系統均需安裝防毒軟體，且掃毒引擎與病毒碼應設定可自動更新至最新版本，或採用中控台派送核可更新檔；若未安裝防毒軟體應輔以其他控制。
 | ○ | **○** | ○ |  |
| 1. 安裝防毒軟體之主機和個人電腦應啟動即時病毒防範機制，並依排程週期執行完整掃描。
 | ○ | **○** | ○ |  |
| 1. 專案辦理活動而蒐集與處理之個人資料，應以最小範圍為原則，並於目的結束後刪除，相關資訊均須函送本會備查。
 | ○ | **○** | ○ |  |
| 1. 上線前應清除正式環境之測試資料及相關測試帳號。
 | ○ | **○** |  |  |
| 1. 承商應配合本會執行弱點掃瞄與滲透測試修補作業，屬於「高風險」之弱點應依據弱掃報告或匯整於「弱點處理報告表」列管，並於一個月內改善。
 | ○ | **○** |  | 填寫「弱點處理報告表」 |
| 1. 承商應每季定期提供容量監控資訊，至少包含CPU、記憶體、硬碟空間。
 | ○ | **○** |  |  |
| 1. 營運環境的作業系統禁止安裝非法軟體或惡意軟體。
 | ○ | **○** | ○ |  |
| 1. 專案執行期間如遇本會資訊安全管理制度規範新增或修訂，承商接獲通知後應配合執行。
 | ○ | **○** | ○ |  |
| 四、存取控制安全要求 |
| 1. 承商不得使用本會設備和網路服務，連接可能損害本會聲譽的網站或從事非法行為。
 | ○ | **○** | ○ |  |
| 1. 承商因業務需要取得本會機敏等級之資料，採電子型式於外部分送時，應使用軟體(如Office或ZIP等)進行加密。
 | ○ | **○** | ○ |  |
| 1. 有關敏感資訊之儲存應考量最小化需求，敏感資訊之輸入應使用適當之遮罩或隱碼措施，傳輸與儲存過程加密保護，並定期檢討加密機制之有效性。
 | ○ | **○** | ○ |  |
| 五、資安事件通報與應變處置 |
| 1. 發現疑似資訊安全或個資外洩等異常事件或事故時，有責任即時通報本會承辦人員，並提供資安事件或事故相關資訊。
 | ○ | **○** | ○ |  |
| 1. 於接獲通報時間起1小時內應完成以下事項：
2. 關閉資通系統對外服務(勿關機)
3. 向雲端資料中心申請全系統當下快照服務，及最近三代快照之檔案
4. 承商應委請資安專業承商進行事件鑑識
5. 於國家資通安全資通應變網站 (<https://www.ncert.nat.gov.tw/>)文件下載區，填寫「資通安全事件通報單」通報階段(P2~4)，寄送至本會系統承辦人。
 | ○ | **○** | ○ | 填寫「資通安全事件通報單」之通報階段 |
| 1. 於接獲通報時間起24小時內應完成事件損害控制或復原程序，至少包含以下事項：
2. 進行事件分析、封鎖及圍堵。
3. 承商提供更名之惡意程式檔及對應之雜湊值(如：MD5和SHA1編碼)，和惡意IP或網址，並保留跡證供後續追查。
4. 依據事件分類(如:網頁攻擊、非法入侵、DDoS阻斷服務、設備問題)填寫「資通安全事件通報單」之應變處置階段，寄送至本會系統承辦人。
 | ○ | **○** | ○ | 填寫「資通安全事件通報單」之應變處置階段 |
| 1. 於接獲通報時間起20日內應完成事件結報程序，完成調查、處理及改善報告，內容包含：
2. 事件發生或知悉其發生、完成損害控制或復原作業之時間。
3. 事件影響之範圍及損害評估。
4. 損害控制及復原作業之歷程。
5. 事件調查及處理作業之歷程。
6. 事件根因分析。
7. 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。
8. 前款措施之預定完成時程及成效追蹤機制。
 | ○ | **○** | ○ | 填寫「資通安全事件通報單」之結報階段 |
| 六、交付文件 |
| 1. 工作計畫應包含資通安全管理措施，如有分包，則一併敘明分包廠商之資通安全維護措施並附上「分包承商清單」。
 | ○ | **○** | ○ |  |
| 1. 資通系統防護基準控制措施報告
 | ○ | **○** |  |  |
| 1. 本專案政府組態基準(Government Configuration Baseline，簡稱GCB)套用報告，如有例外應連同GCB例外管理清單一併交付
 | ○ | **○** |  |  |
| 1. 資產清冊
 | ○ | **○** |  |  |
| 1. 系統套件清單及證明文件
 | ○ | **○** | ○ | 型一和型二：交付「系統套件清單」型三：交付使用授權證明。 |
| 1. 備份政策管理表
 | ○ | **○** | ○ | 型三：請說明Saas備份政策 |

貳、附表：

1. 資通系統防護基準自評表
2. 系統套件清單
3. 備份政策管理表
4. GCB例外管理清單
5. 資訊資產清冊
6. 弱點處理報告表
7. 資通安全事件通報單

|  |  |
| --- | --- |
| 附表一、資通系統防護基準自評表 |  |
| 資通系統防護基準自評表（填表日期： 年 月 日） |  |
| 資訊系統名稱 | 　 | 承辦人 | 　 | e-mail： |
| 委外廠商名稱 | 　 | 廠商代表 | 　 | e-mail： |
| 安全等級評估表(請以■標示) | 1.機密性：□普　□中　□高。　2.完整性：□普　□中　□高。　3.可用性：□普　□中　□高。　4.法律遵循性：□普　□中　□高。 |
| 安全類型 | 措施內容 | 系統防護需求 | 普 | 中 | 高 | 符合性評估 | 說明現有控制措施 | 參考補充說明 |
| 存取控制 | 帳號管理 | 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。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 管理者和使用者依據「ISMS-B.05 存取安全管理要點」要求，應填具「ISMS-D.B.05-01 帳號新增異動申請表」並經審核通過。 |
| 存取控制 | 帳號管理 | 已逾期之臨時或緊急帳號應刪除或禁用。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 每年針對應用系統帳號權限進行清查，針對臨時或緊急帳號進行刪除或禁用。 |
| 存取控制 | 帳號管理 | 資通系統閒置帳號應禁用。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 應定期盤點系統未使用之帳號(如:超過1年)，其包含人員/系統所使用之帳號 |
| 存取控制 | 帳號管理 | 定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 依據「ISMS-B.05 存取安全管理要點」每年定期執行帳號權限清查，範圍包含:網路設備、防火牆、資料庫、作業系統、應用系統後台等帳號清查作業，並填寫「ISMS-D.B.05-02 使用者帳號清單」審核備查。 |
| 存取控制 | 帳號管理 | 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。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 應按GCB規範要求，逾時15分鐘即強制登出 |
| 存取控制 | 帳號管理 | 應依機關規定之情況及條件，使用資通系統。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 依據「ISMS-B.05 存取安全管理要點」要求，包含：遠距工作管理SSL VPN.。 |
| 存取控制 | 帳號管理 | 監控資通系統帳號，如發現帳號違常使用時回報管理者。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 應啟用事件檢視器之帳號登入登出留存，並以自動/定期方式檢視或監控。 |
| 存取控制 | 最小權限 | 採最小權限原則，僅允許使用者(或代表使用者行為的程序)依據機關任務和業務功能，完成指派任務所需之授權存取。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 本系統依據機關任務和業務功能，完成指派任務所需之授權存取。 |
| 存取控制 | 遠端存取 | 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 。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 依據「ISMS-C.B.08-01 防火牆建置與管理作業程序」，另廠商遠端連線SSLVPN申請流程辦理。 |
| 存取控制 | 遠端存取 | 應監控資通系統遠端連線。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 依據「ISMS-C.B.08-01 防火牆建置與管理作業程序」，另廠商遠端連線SSLVPN申請流程辦理。 |
| 存取控制 | 遠端存取 | 資通系統應實作加密機制。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 應使用GCB規範之加密機制，包含但不限於憑證使用。 |
| 存取控制 | 遠端存取 | 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。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 依據「ISMS-C.B.08-01 防火牆建置與管理作業程序」，另廠商遠端連線SSLVPN申請流程辦理。 |
| 稽核與可歸責性 | 稽核事件 | 依規定時間週期及紀錄留存政策，保留稽核紀錄。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 依據本會「ISMS-B.07 作業安全管理要點」規範，資訊設備與系統之紀錄(包含Event Log應保留至少半年(個人資料檔案存取相關紀錄應至少保留5年以上)，若無法線上保存，則應將紀錄匯出存檔備查。 |
| 稽核與可歸責性 | 稽核事件 | 確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 資通系統有稽核特定事件之功能，包含登入失敗歷程、執行功能操作時，發生作業失敗的歷程。 |
| 稽核與可歸責性 | 稽核事件 | 應稽核資通系統管理者帳號所執行之各項功能。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 每年針對應用系統帳號權限進行清查，稽核資通系統管理者帳號所執行之各項功能，啟用管理者稽核功能。 |
| 稽核與可歸責性 | 稽核事件 | 應定期審查稽核事件 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 應定期(例如:每周或每月)檢視紀錄是否有異常情事。以Ｗindows為例，檢視事件檢視器日誌，開始-->控制台->系統管理工具->事件檢視器以Linux(CentOS)為例，檢視系統登入成功、失敗紀錄(/var/log/secure) |
| 稽核與可歸責性 | 稽核紀錄內容 | 資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式的一致性。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | LOG內容包含登入帳號、登入時間之稽核軌跡。以Ｗindows為例，檢視與調整稽核原則，控制台->系統管理工具->本機安全性設定值->本機原則->稽核原則 |
| 稽核與可歸責性 | 稽核紀錄內容 | 資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | LOG內容包含登入帳號、登入時間之稽核軌跡。以Ｗindows為例，檢視與調整稽核原則，控制台->系統管理工具->本機安全性設定值->本機原則->稽核原則 |
| 稽核與可歸責性 | 稽核儲存容量 | 依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 應配置適當儲存容量、或額外以log server方式留存稽核軌跡，至少保存1年以上，敏感性資料(含個資)至少保存5年以上。 |
| 稽核與可歸責性 | 稽核處理失效之回應 | 資通系統於稽核處理失效時，應採取適當之行動。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 備份空間達80%時，維運廠商將通報承辦人，待承辦人進行後續指示。 |
| 稽核與可歸責性 | 稽核處理失效之回應 | 機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 維運廠商將通報承辦人，待承辦人進行後續指示。 |
| 稽核與可歸責性 | 時戳及校時 | 資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | NTP校時 |
| 稽核與可歸責性 | 時戳及校時 | 系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | NTP校時 |
| 稽核與可歸責性 | 稽核資訊之保護 | 對稽核紀錄之存取管理，僅限於有權限之使用者。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 系統負責人、系統廠商及可讀取LOG，其餘使用者無權限。 |
| 稽核與可歸責性 | 稽核資訊之保護 | 應運用雜湊或其他適當方式之完整性確保機制。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 考量使用雜湊函數進行完整性比對 |
| 稽核與可歸責性 | 稽核資訊之保護 | 定期備份稽核紀錄至與原稽核系統不同之實體系統。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 確認稽核紀錄留存方式及是否設有LOG Server機制備份留存 |
| 營運持續計畫 | 系統備份 | 訂定系統可容忍資料損失之時間要求。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 　 |
| 營運持續計畫 | 系統備份 | 執行系統源碼與資料備份。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 每次版本更新時應定期備份系統之原始碼與定期資料庫備份 |
| 營運持續計畫 | 系統備份 | 應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 依據「ISMS-B.07-02 備份政策管理表」執行備份，每年至少 執行一次備份還原演練測試 |
| 營運持續計畫 | 系統備份 | 應將備份還原，作為營運持續計畫測試之一部分。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 資通系統每年擇一情境，填寫「ISMS-D.B.12-02 營運持續計畫演練紀錄表」辦理營運持續計畫測試演練，並包含備份還原演練。 |
| 營運持續計畫 | 系統備份 | 應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 應依照服務性質實施網段區隔 |
| 營運持續計畫 | 系統備援 | 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 訂定可容忍中斷時間 |
| 營運持續計畫 | 系統備援 | 原服務中斷時，於可容忍時間內，由備援設備取代提供服務。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 備援機制或HA架構 |
| 識別與鑑別 | 內部使用者之識別與鑑別 | 資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 如 專人專帳 SSO驗證等 |
| 識別與鑑別 | 內部使用者之識別與鑑別 | 對帳號之網路或本機存取採取多重認證技術。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 如OTP等 |
| 識別與鑑別 | 身分驗證管理 | 使用預設密碼登入系統時，應於登入後要求立即變更。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 　 |
| 識別與鑑別 | 身分驗證管理 | 身分驗證相關資訊不以明文傳輸。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | HTTPS加密傳輸 |
| 識別與鑑別 | 身分驗證管理 | 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五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。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | GCB以Ｗindows為例，檢視與調整稽核原則，控制台->系統管理工具->安全性設定->帳戶原則->帳戶鎖定原則 |
| 識別與鑑別 | 身分驗證管理 | 基於密碼之鑑別資通系統應強制最低密碼複雜度;強制密碼最短及最長之效期限制。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | GCB以Ｗindows為例，檢視與調整稽核原則，控制台->系統管理工具->安全性設定->帳戶原則->密碼原則 |
| 識別與鑑別 | 身分驗證管理 | 使用者更換密碼時，至少不可以與前三次使用過的密碼相同。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | GCB以Ｗindows為例，檢視與調整稽核原則，控制台->系統管理工具->安全性設定->帳戶原則->密碼原則 |
| 識別與鑑別 | 身分驗證管理 | 對非內部使用者，可依機關自行規範密碼設定強度、效期與密碼不重複次數。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | GCB以Ｗindows為例，檢視與調整稽核原則，控制台->系統管理工具->安全性設定->帳戶原則->密碼原則 |
| 識別與鑑別 | 身分驗證管理 | 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 設置密碼錯誤即鎖定機制 |
| 識別與鑑別 | 身分驗證管理 | 密碼重設機制對使用者新身分確認後，發送一次性及具有時效符記。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | Token/Session不可永久有效，應於每次重新認證時配發 |
| 識別與鑑別 | 鑑別資訊回饋 | 資通系統應遮蔽鑑別過程中之資訊。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 視資料機敏程度執行加密或遮罩 |
| 識別與鑑別 | 加密模組鑑別 | 資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 密碼儲存於資料庫時，不應以明碼方式儲存 |
| 識別與鑑別 | 非內部使用者之識別與鑑別 | 資通系統應識別及鑑別非機關使用者 (或代表機關使用者行為之程序 )。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與服務獲得 | 系統發展生命週期需求階段 | 針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 1. 依據資通安全管理法子法附錄之資通系統分級及防護基準要求，針對資通系統之機密性、完整性、可用性與法律遵行性，填寫「安全等級評估表」及「資通系統防護基準表」。2. 後續將依內部稽核檢查表，查核資通系統之機密性、完整性及可用性，應至少符合防護基準控制項目之要求 |
| 系統與服務獲得 | 系統發展生命週期設計階段 | 根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 每年針對資通相關設備與系統進行風險評鑑，並針對風險進行處理。 |
| 系統與服務獲得 | 系統發展生命週期設計階段 | 將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 每年針對資通相關設備與系統進行風險評鑑，並針對風險進行處理。 |
| 系統與服務獲得 | 系統發展生命週期開發階段 | 應針對安全需求實作必要控制措施。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 資通系統契約皆有要求開發者(廠商)於該系統程式開發過程遵循相關規範。 |
| 系統與服務獲得 | 系統發展生命週期開發階段 | 應注意避免軟體常見漏洞及實作必要控制措施。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 請參考最新OWASP TOP 10  |
| 系統與服務獲得 | 系統發展生命週期開發階段 | 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。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 應設置error page |
| 系統與服務獲得 | 系統發展生命週期開發階段 | 執行「源碼掃描」安全檢測。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與服務獲得 | 系統發展生命週期開發階段 | 具備系統嚴重錯誤之通知機制。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與服務獲得 | 系統發展生命週期測試階段 | 執行「弱點掃描」安全檢測。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與服務獲得 | 系統發展生命週期測試階段 | 執行「滲透測試」安全檢測。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與服務獲得 | 系統發展生命週期部 署與維運階段 | 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。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 應以最小需求為原則啟用必要服務與埠口 |
| 系統與服務獲得 | 系統發展生命週期部 署與維運階段 | 資通系統相關軟體，不使用預設密碼。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 所有預設密碼應於首次啟用時立即變更 |
| 系統與服務獲得 | 系統發展生命週期部 署與維運階段 | 於系統發展生命週期之維運階段，須注意版本控制與變更管理。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 請確認版本控制方式、使用軟體及版控權限是否妥適 |
| 系統與服務獲得 | 系統發展生命週期委外階段 | 資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求 （含機密性、可用完整） 納入委外契約。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與服務獲得 | 獲得程序 | 開發、測試及正式作業環境應為區隔。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 資通系統開發網段：資通系統測試區網段：資通系統營運區網段： |
| 系統與服務獲得 | 系統文件 | 應儲存與管理系統發展生命週期之相關文件。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 系統維運廠商應定期交付系統發展生命週期之相關文件。 |
| 系統與通訊保護 | 傳輸之機密性與完整性 | 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。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 應強制使用TLS1.1以上之加密機制 |
| 系統與通訊保護 | 傳輸之機密性與完整性 | 使用公開、國際機構驗證且未遭破解之演算法。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 不可使用弱加密，如DES等 |
| 系統與通訊保護 | 傳輸之機密性與完整性 | 支援演算法最大長度金鑰。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 應排除使用已知遭破解之弱金鑰與雜湊函數 |
| 系統與通訊保護 | 傳輸之機密性與完整性 | 加密金鑰或憑證週期性更換。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與通訊保護 | 傳輸之機密性與完整性 | 伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 包括金鑰生命週期之管理、憑證管理、資料加密金鑰、認證金鑰均應納入 |
| 系統與通訊保護 | 資料儲存之安全 | 靜置資訊及相關具保護需求之機密資訊應加密儲存。註:靜置資訊，指資訊位於資通系統特定元件，例如儲存設備上之狀態，或與系統相關需要保護之資訊，例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與資訊完整性 | 漏洞修復 | 系統之漏洞修復應測試有效性及潛在影響，並定期更新。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與資訊完整性 | 漏洞修復 | 定期確認資通系統相關漏洞修復之狀態。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 包含但不限於作業系統、系統伺服器、組建、函式庫、韌體等 |
| 系統與資訊完整性 | 資通系統監控 | 發現資通系統有被入侵跡象時，應通報機關特定人員。 | ★ | ★ | ★ | □符合□不符合□不適用 | 　 | 應依據本會「ISMS-B.11 資訊安全事故管理要點」通報並填寫「資通安全事件通報單」 |
| 系統與資訊完整性 | 資通系統監控 | 監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與資訊完整性 | 資通系統監控 | 資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與資訊完整性 | 軟體及資訊完整性 | 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 可考慮採行雜湊方式驗證 |
| 系統與資訊完整性 | 軟體及資訊完整性 | 使用者輸入資料合法性檢查應置放於應用系統伺服器端。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 每次寫入時應執行驗證檢查 |
| 系統與資訊完整性 | 軟體及資訊完整性 | 發現違反完整性時，資通系統應實施機關指定之安全保護措施。 | 　 | ★ | ★ | □符合□不符合□不適用 | 　 | 　 |
| 系統與資訊完整性 | 軟體及資訊完整性 | 應定期執行軟體與資訊完整性檢查。 | 　 | 　 | ★ | □符合□不符合□不適用 | 　 | 可考慮採行雜湊方式驗證 |

附表二、系統套件清單

系統套件清冊

清點日期：

|  |  |
| --- | --- |
| 系統名稱 |  |
| 單位名稱 |  | 承辦人 |  |
| 委外廠商名稱 |  | 委外廠商聯絡窗口 |  |

※非自行開發套件

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 編號 | 軟體套件名稱 | 版本 | 授權證書編號 (證明) | 來源(如:網址) | 用途說明 | 授權書保管者 | 安裝實體位置 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

※ 其它授權軟體(OS、DB、Other)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 編號 | 軟體名稱 | 版本 | 數量 | 授權證書編號 (證明) | 用途說明 | 授權書保管者 | 安裝實體位置 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 填表人 | 承辦人 | 科長 |
|  |  |  |

附表三、備份政策管理表

**備份政策管理表**

更新日期： / /

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **應用系統名稱** | **系統管理人員** | **主機名稱** | **備份範圍** | **資料備份方式與週期** | **備份時間** | **備份方式** | **網路備份路徑** | **備註** |
|  |  |  |  | □差異:每\_\_\_備份□增量:每\_\_\_備份□完整:每\_\_\_備份 |  | □磁帶□其他： |  |  |
|  |  |  |  | □差異:每\_\_\_備份□增量:每\_\_\_備份□完整:每\_\_\_備份 |  | □磁帶□其他： |  |  |
|  |  |  |  | □差異:每\_\_\_備份□增量:每\_\_\_備份□完整:每\_\_\_備份 |  | □磁帶□其他： |  |  |
|  |  |  |  | □差異:每\_\_\_備份□增量:每\_\_\_備份□完整:每\_\_\_備份 |  | □磁帶□其他： |  |  |
|  |  |  |  | □差異:每\_\_\_備份□增量:每\_\_\_備份□完整:每\_\_\_備份 |  | □磁帶□其他： |  |  |
|  |  |  |  | □差異:每\_\_\_備份□增量:每\_\_\_備份□完整:每\_\_\_備份 |  | □磁帶□其他： |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 承辦人 |  | 科長 |  |

附表四、GCB例外管理清單

|  |
| --- |
| 【OOO資通系統】GCB例外管理 |
| 項次 | TWGCB-ID | 規則名稱 | 基準值 | 變更值 | 變更理由 | 配套措施 | 適用範圍 |
| 範例 | TWGCB-01-005-0002 | 密碼最長使用期限 | 90天以下 | 180天 | 提供對一般民眾使用，為不造成民眾困擾，故暫時保留原設定值 | 增加密碼的長度與複雜度，將密碼長度調整為10個字元，與密碼必須符合複雜性需求，提供密碼安全性 | 本系統前台登入機制 |
| 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
|  |  |  |  |  |  |  |  |
| 承辦人 | 審核人 | 核准日期 |  |  |  |
| 　 | 　 | 　 |  |  |  |

附表五、資訊資產清冊

|  |
| --- |
| 1.資產大類共分5類包含人員類、資訊類、軟體類、硬體類及服務類。2.擁有者 : 依據本會ISMS-B.02 資產管理要點定義為負責管理資產盤點與價值評估作業，核准所轄資產之存取權限，並規劃資產分類、分級、使用、分送複製、保存及銷毀作業方式。3.機密性、完整性及可用性請依據資通系統三面向分級結果對應至此表(普為1分、中為3分、高為5分)4.資產價值 : 為機密性、完整性及可用性之分數相乘 |
| **項次** | **資產名稱** | **資產大類** | **擁有者/職位(內部人員)** | **管理者(部門)** | **使用者** | **存放位置** | **資產說明/備註** | **機密性** | **完整性** | **可用性** | **資產價值** | **資訊系統服務或資訊作業流程** |
| 1 | 　 | 　 | 　 | 　 | 　 | 　 | 使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。使用 SHIFT+ENTER 來開啟功能表 (新視窗)。 | 　 | 　 | 　 | 　 | 　 |
| 2 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 3 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 4 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 5 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 6 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 7 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 8 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 9 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 10 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 11 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 12 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 13 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 14 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 15 |  |  |  |  |  |  |  |  |  |  |  |  |

附表六、弱點處理報告表

弱點處理報告表

| 設備名稱： | IP位址： | 管理人員： | 日期： 年 月 日 |
| --- | --- | --- | --- |
| 編號 | 弱點名稱 | 等級 | 修補作業說明 | 修補完成日期 | 無法修補原因與防禦因應方法 | 追蹤/覆核人員 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

備註：追蹤或覆核人員應確認修補作業、無法修補原因與防禦因應方法之適切性

|  |  |  |  |
| --- | --- | --- | --- |
| 承辦人 |  | 科長 |  |

附表七、資通安全事件通報單

**資通安全事件通報單**

一、遵照資通安全管理法，公務機關與特定非公務機關發生資安事件時，應於限定時間內辦理事件通報、損害控制或復原通知，並於完成事件損害控制或復原後一個月內完成資通安全事件調查、處理及改善報告。

二、公務機關、公營事業或政府捐助之財團法人應至國家資通安全通報應變網站（https://www.ncert.nat.gov.tw）通報資安事件，若因故無法上網填報，可先填具本通報單以傳真或郵寄方式傳送至國家資通安全會報政府資通安全組，俟網路連線恢復後，仍須至通報應變網站進行資安事件補登作業。

傳真專線：(02)27331655

郵寄地址：台北市大安區106富陽街116號

諮詢專線：(02)27339922

三、資通安全事件通報單填寫注意事項如下：

1.「◎」為必填項目。

2.請依通報之資安「事件分類」填寫通報單，並依事件類別回傳通報單內容。

3.事件通報的部分請回傳P2-P4

4.事件損害控制或復原的部分請根據事件分類回傳對應的頁碼

 (網頁攻擊P2-P6、非法入侵P2-P4,P9-P10、阻斷服務P2-P4, P13、

 設備問題P2-P4, P16、其他P2-P4, P19-P20)

5.事件調查處理及改善報告的部分請根據事件分類回傳對應的頁碼

(網頁攻擊P2-P8、非法入侵P2-P4,P9-P12、阻斷服務P2-P4, P13-P15、

 設備問題P2-P4, P16-P18、其他P2-P4, P19-P22)

|  |
| --- |
| **【壹、事件通報】(通報階段)** |
| ◎填報時間：\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |
| **STEP1.請填寫事件相關基本資料** |
| 一、發生資通安全事件之機關(機構)聯絡資料：◎機關(機構)名稱：　　　　　　　　　◎審核機關名稱：　　　　　　　　　　　◎通報人：　　　　　 　 ◎電話：　　　　　 傳真：　　　　　　 ◎電子郵件信箱：　　　　　　 ◎是否代其他機關(構)通報：🌕是，該單位名稱 🌕否◎資安事件調查廠商：  |
| **STEP2.請詳述事件發生過程** |
| 二、事件發生過程：◎事件發現時間：\_\_\_\_\_年\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分◎事件分類與異常狀況：(事件分類為單選項；異常狀況為複選項)🌕網頁攻擊  □網頁置換 □惡意留言 □惡意網頁 □釣魚網頁 □網頁木馬 □網站個資外洩🌕非法入侵 □系統遭入侵 □植入惡意程式 □異常連線 □發送垃圾郵件 □資料外洩 🌕阻斷服務(DoS/DDoS) □服務中斷 □效能降低🌕設備問題 □設備故障/毀損 □電力異常 □網路服務中斷 □設備遺失🌕其他：　　　　　\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎事件說明及影響範圍 【請說明事件發生經過，如機關如何發現此事件、處理情形等】 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎是否影響其他政府機關(構)或重要民生設施運作：🌕是 🌕否◎承上，影響機關(構)/重要民生設施領域名稱： □水資源 □能源 □通訊傳播 □交通 □銀行與金融  □緊急救援與醫院 □重要政府機關 □高科技園區◎此事件通報來源：🌕自行發現 🌕警訊通知，發布編號：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 🌕其他外部情資：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **STEP3.評估事件影響等級** |
| 三、事件影響等級：◎請分別評估資安事件造成之機密性、完整性以及可用性衝擊：\*資安事件影響等級為機密性、完整性及可用性衝擊最嚴重者(數字最大者)－機密性衝擊：（單選）🌕一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊 遭嚴重洩漏，或國家機密資料遭洩漏(4級) 🌕未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務 機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩 漏(3級) 🌕非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業  務資訊遭輕微洩漏(2級) 🌕非核心業務資訊遭輕微洩漏(1級) 🌕無資料遭洩漏(無需通報) －完整性衝擊：（單選）🌕一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊 或核心資通系統遭嚴重竄改，或國家機密遭竄改(4級)🌕未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重 竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改(3級)🌕非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改(2級)🌕非核心業務資訊或非核心資通系統遭輕微竄改(1級)🌕無系統或資料遭竄改(無需通報) －可用性衝擊：（單選）🌕涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響 或停頓，無法於可容忍中斷時間內回復正常運作(4級)🌕未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作(3級)🌕非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作(2級)🌕非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響(1級)🌕無系統或設備運作受影響(無需通報) |
| **Step4.評估是否需要外部支援** |
| 四、期望支援項目：  ◎是否需要支援：🌕是（請續填期望支援內容） 🌕否（免填期望支援內容） 期望支援內容：（請勿超過200字） \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |
| --- |
| **【貳、損害控制或復原-網頁攻擊】(應變處置階段)** |
| **Step5.請填寫機關緊急應變措施-網頁攻擊**(請回傳P2-P6) |
| 五、完成損害控制或復原：◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處罝說明」欄位說明)* 已保存遭入侵主機事件紀錄檔〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存防火牆紀錄〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存網站日誌檔〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共\_\_\_\_\_個
* 其他保留資料或資料處罝說明【如未保存資料亦請說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)，經分析已保存之紀錄，是否發現下列異常情形：* 異常連線行為【請列出異常IP與異常連線原因，如：存取後台管理頁面】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 異常帳號使用【請列出帳號並說明帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 清查網頁目錄內容，網站內存在未授權之程式/檔案【請說明程式名稱或路徑、檔名】

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 網站資料庫內容遭竄改
* 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 影響評估說明補充【請填寫補充說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)因應分析結果，執行處置措施：* 移除未授權存在之惡意網頁/留言/檔案，共\_\_\_\_筆**(必填)**

 【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 將異常外部連線IP列入阻擋清單**(必填)**【請說明設定阻擋之資訊設備與阻擋之IP，如無須阻擋，請填寫「無」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 停用/刪除異常帳號**(必填)**【請說明停用/刪除之帳號，如無須刪除，請填寫「無」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 移除網站外洩資料
* 通知事件相關當事人，並依內部資安通報作業向上級呈報
* 暫時中斷受害主機網路連線行為至主機無安全性疑慮
* 已向搜尋引擎提供者申請移除庫存頁面〈複選〉《□Google□Yahoo□Yam(蕃薯藤) □Bing□Hinet

□其他搜尋引擎提供者\_\_\_\_\_\_\_\_\_》* 修改網站程式碼，並檢視其他網站程式碼，完成日期\_\_\_\_\_\_\_\_\_\_
* 重新建置作業系統與作業環境，完成日期\_\_\_\_\_\_\_\_\_\_\_\_\_
* 應變措施補充說明【請填寫補充說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎應變處置綜整說明【請說明損害控制或復原之執行狀況】： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  是否已完成損害控制或復原 🌕否，尚未完成損害控制或復原 🌕是，已完成損害控制 🌕是，已完成損害控制並復原  完成損害控制或復原時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |

|  |
| --- |
| **【參、調查、處理及改善報告-網頁攻擊】(結報階段)** |
| **STEP6.資安事件結案作業-網頁攻擊**(請回傳P2-P8) |
| 六、事件調查與處理： ◎受害資訊設備數量：電腦總計\_\_\_\_\_\_\_臺；伺服器總計\_\_\_\_\_\_\_臺； 其他設備\_\_\_\_\_\_\_ 總計\_\_\_\_\_\_\_臺 ◎IP位址(IP Address)(無；可免填)外部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 內部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎網際網路位址（Web-URL）(無；可免填)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎作業系統名稱、版本：🌕Windows系列 🌕Linux系列 🌕其他作業平台 版本：\_\_\_\_\_\_\_\_\_\_\_\_◎受害系統是否通過資安管理認證(ISMS)：🌕是 🌕否◎資安監控中心(SOC)：🌕無 🌕機關自行建置  🌕委外建置，該廠商名稱 ◎受害主機是否納入SOC監控範圍：🌕是 🌕否◎機關是否裝置資安防護設備：🌕是 🌕否(不須填寫資安防護類型) 資安防護類型〈複選〉〈□防毒軟體，監控設備代號：  □網路防火牆，監控設備代號：  □電子郵件過濾機制，監控設備代號：  □入侵偵測及防禦機制，監控設備代號：  □應用程式防火牆，監控設備代號：  □進階持續性威脅攻擊防禦措施，監控設備代號：  □其他，監控設備代號： 〉◎SOC業者是否發送事件告警資訊：🌕是 🌕否(不須填寫情資分析單編號) 情資單分析編號： ◎事件發生原因〈單選〉〈🌕作業系統漏洞 🌕弱密碼 🌕應用程式漏洞 🌕網站設計不當 🌕人為疏失 🌕設定錯誤 🌕廠商維護環境或管理疏失 🌕無法確認事件原因《🌕無相關紀錄檢視🌕相關紀錄遭異常刪除/變更  🌕受限於資安人力/預算無法調查🌕逕行重建無法調查🌕系統汰換逕 行下架🌕事件調查後仍無法確認原因》🌕其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_〉 ◎請簡述事件處理情況：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎補強措施〈複選〉* + - 1. 補強系統/程式安全設定
				* 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等)**(必填)**
				* 已完成評估變更受害主機中所有帳號之密碼(含本機管理者) **(必填)**
				* 已完成檢視/更新受害主機系統與所有應用程式至最新版本(包含網站編輯管理程式，如：FrontPage) **(必填)**【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* + - * + 關閉網路芳鄰功能
				+ 設定robots.txt檔，控制網站可被搜尋頁面
				+ 已針對所有需要特殊存取權限之網頁加強身分驗證機制【請說明機制名稱或類別】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* + - * + 限制網站主機上傳之附件檔案類型【請說明附檔名】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* + - * + 限制網頁存取資料庫的使用權限，對於讀取資料庫資料的帳戶身分及權限加以管制
				+ 限制連線資料庫之主機IP
				+ 關閉WebDAV(Web Distribution Authoring and Versioning)
			1. 資安管理與教育訓練
				* 重新檢視機關網路架構適切性
				* 機關內部全面性安全檢測
				* 加強內部同仁資安教育訓練
				* 修正內部資安防護計畫

◎其他相關安全處置【請填寫相關處置、預定完成時程及成效追蹤機制】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎調查、處理及改善報告繳交(登錄結報)時間：\_\_\_\_\_\_\_年\_\_\_\_\_\_\_月\_\_\_\_\_\_日\_\_\_\_\_\_時\_\_\_\_\_\_分 |

|  |
| --- |
| **【貳、損害控制或復原-非法入侵】(應變處置階段)** |
| **Step5.請填寫機關緊急應變措施-非法入侵**(請回傳P2-P4、P9-P10) |
| 五、完成損害控制與復原：◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處罝說明」欄位說明) * 已保存遭受害主機事件紀錄檔〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存防火牆紀錄〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共\_\_\_\_\_個
* 其他保留資料或資料處罝說明【如未保存資料亦請說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)經分析已保存之紀錄，是否發現下列異常情形：* 異常連線行為【請列出異常IP與異常連線，如：存取後台管理頁面】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 異常帳號使用【請列出帳號並說帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 影響評估補充說明【請填寫補充說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)因應分析結果，執行處置措施：* 移除未授權存在之惡意網頁/留言/檔案/程式，共\_\_\_\_\_筆**(必填)**

 【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 將可疑IP/Domain Name列入阻擋清單**(必填)**【請說明設定阻擋之資訊設備與阻擋之IP，如無須阻擋，請填寫「無」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 停用/刪除異常帳號**(必填)**【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 中斷受害主機網路連線行為至主機無安全性疑慮
* 重新建置作業系統與作業環境，完成日期
* 惡意程式樣本送交防毒軟體廠商，共\_\_\_\_\_個
* 應變措施補充說明【請填寫補充說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎應變處置綜整說明【請說明損害控制或復原之執行狀況】： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  是否已完成損害控制或復原 🌕否，尚未完成損害控制或復原 🌕是，已完成損害控制 🌕是，已完成損害控制並復原完成損害控制或復原時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |

|  |
| --- |
| **【參、調查、處理及改善報告-非法入侵】(結報階段)** |
| **Step6.資安事件結案作業-非法入侵**(請回傳P2-P4、P9-P12) |
| 六、事件調查與處理： ◎受害資訊設備數量：電腦總計\_\_\_\_\_\_\_臺；伺服器總計\_\_\_\_\_\_\_臺； 其他設備\_\_\_\_\_\_\_ 總計\_\_\_\_\_\_\_臺 ◎IP位址(IP Address)(無；可免填)外部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 內部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎網際網路位址（Web-URL）(無；可免填)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎作業系統名稱、版本：🌕Windows系列 🌕Linux系列 🌕其他作業平台 版本：\_\_\_\_\_\_\_\_\_\_\_\_◎受害系統是否通過資安管理認證(ISMS)：🌕是 🌕否◎資安監控中心(SOC)：🌕無 🌕機關自行建置  🌕委外建置，該廠商名稱 ◎受害主機是否納入SOC監控範圍：🌕是 🌕否◎機關是否裝置資安防護設備：🌕是 🌕否(不須填寫資安防護類型) 資安防護類型〈複選〉〈□防毒軟體，監控設備代號：  □網路防火牆，監控設備代號：  □電子郵件過濾機制，監控設備代號：  □入侵偵測及防禦機制，監控設備代號：  □應用程式防火牆，監控設備代號：  □進階持續性威脅攻擊防禦措施，監控設備代號：  □其他，監控設備代號： 〉◎SOC業者是否發送事件告警資訊：🌕是 🌕否(不須填寫情資分析單編號) 情資單分析編號： ◎事件發生原因〈單選〉〈🌕社交工程🌕作業系統漏洞🌕弱密碼🌕應用程式漏洞🌕網站設計不當 🌕廠商維護環境或管理疏失 🌕無法確認事件原因《🌕無相關紀錄檢視 🌕相關紀錄遭異常刪除/變更🌕受限於資安人力/預算無法調查🌕逕行重 建無法調查🌕系統汰換逕行下架🌕事件調查後仍無法確認原因》 🌕其他\_\_\_\_\_\_\_\_\_\_\_〉【請說明事件調查情況】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎補強措施〈複選〉1. 補強系統/程式安全設定〈複選〉
	* + - * 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等) **(必填)**
				* 已完成評估變更受害主機中所有帳號密碼之必要性(含本機管理者) **(必填)**
				* 已完成檢視/更新受害主機系統與所有應用程式至最新版本**(必填)**【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* + - * + 關閉郵件伺服器Open Relay功能
				+ 關閉網路芳鄰功能
1. 資安管理與教育訓練(複選)
	* + - * 重新檢視機關網路架構適切性
				* 機關內部全面性安全檢測
				* 加強內部同仁資安教育訓練
				* 修正內部資安防護計畫

◎其他相關安全處置【請填寫相關處置、預定完成時程及成效追蹤機制】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎調查、處理及改善報告繳交(登錄結報)時間：\_\_\_\_\_\_\_年\_\_\_\_\_\_\_月\_\_\_\_\_\_日\_\_\_\_\_\_時\_\_\_\_\_\_分 |

|  |
| --- |
| **【貳、損害控制或復原-阻斷服務(DoS/DDoS)】(應變處置階段)** |
| **Step5.請填寫機關緊急應變措施-阻斷服務(DoS/DDoS)** (請回傳P2-P4、P13) |
| 五、完成損害控制與復原：◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處罝說明」欄位說明)* 已保存遭入侵主機事件檢視器〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存防火牆紀錄〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存受攻擊主機封包紀錄〈🌕10分鐘🌕10-30分鐘🌕30-60分鐘〉
* 其他保留資料或資料處罝說明【如未保存資料亦請說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)* 攻擊來源IP數量\_\_\_\_\_\_\_個
* 確認遭攻擊主機用途【請說明主機用途】

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 影響評估補充說明

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)* 阻擋攻擊來源IP**(必填)**【請說明設定阻擋之資訊設備與阻擋之IP，如無須阻擋，請填寫「無」】

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 調整網路頻寬
* 聯繫網路服務提供業者(ISP) (請提供ISP業者名稱)，請其協助進行阻擋
* 應變措施補充說明【請填寫補充說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎應變處置綜整說明【請說明損害控制或復原之執行狀況】： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 是否已完成損害控制或復原 🌕否，尚未完成損害控制或復原 🌕是，已完成損害控制 🌕是，已完成損害控制並復原 完成損害控制或復原時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |

|  |
| --- |
| **【參、調查、處理及改善報告-阻斷服務(DoS/DDoS)】(結報階段)** |
| **Step6.資安事件結案作業-阻斷服務(DoS/DDoS)** (請回傳P2-P4、P13-P15) |
| 六、事件調查與處理： ◎受害資訊設備數量：電腦總計\_\_\_\_\_\_\_臺；伺服器總計\_\_\_\_\_\_\_臺； 其他設備\_\_\_\_\_\_\_ 總計\_\_\_\_\_\_\_臺 ◎IP位址(IP Address)(無；可免填)外部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 內部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎網際網路位址（Web-URL）(無；可免填)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎作業系統名稱、版本：🌕Windows系列 🌕Linux系列 🌕其他作業平台 版本：\_\_\_\_\_\_\_\_\_\_\_\_ ◎受害系統是否通過資安管理認證(ISMS)：🌕是 🌕否◎資安監控中心(SOC)：🌕無 🌕機關自行建置  🌕委外建置，該廠商名稱 ◎受害主機是否納入SOC監控範圍：🌕是 🌕否◎機關是否裝置資安防護設備：🌕是 🌕否(不須填寫資安防護類型) 資安防護類型〈複選〉〈□防毒軟體，監控設備代號：  □網路防火牆，監控設備代號：  □電子郵件過濾機制，監控設備代號：  □入侵偵測及防禦機制，監控設備代號：  □應用程式防火牆，監控設備代號：  □進階持續性威脅攻擊防禦措施，監控設備代號：  □其他，監控設備代號： 〉◎SOC業者是否發送事件告警資訊：🌕是 🌕否(不須填寫情資分析單編號) 情資單分析編號： ◎補強措施〈複選〉1. 補強系統/程式安全設定〈複選〉
	* + - * 已完成檢視/移除主機/伺服器不必要服務功能**(必填)**【請說明服務功能名稱，如無須移除，請填寫「無」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* + - * + 限制同時間單一IP連線
				+ 已完成檢視/更新受害主機系統與所有應用程式至最新版本**(必填)**【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* + - * + DNS主機停用外部遞迴查詢
1. 資安管理與教育訓練〈複選〉
	* + - * 重新檢視機關網路架構適切性
				* 修正內部資安防護計畫

◎其他相關安全處置【請填寫相關處置、預定完成時程及成效追蹤機制】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎調查、處理及改善報告繳交(登錄結報)時間：\_\_\_\_\_\_\_年\_\_\_\_\_\_\_月\_\_\_\_\_\_日\_\_\_\_\_\_時\_\_\_\_\_\_分 |

|  |
| --- |
| **【貳、損害控制或復原-設備問題】(應變處置階段)** |
| **Step5.請填寫機關緊急應變措施-設備問題**(請回傳P2-P4、P16) |
| ◎保留受害期間之相關設備紀錄資料* 其他保留資料或資料處罝說明【如未保存資料亦請說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)* 評估設備影響情況

〈🌕無資料遭損毀 🌕資料損毀，但可由備份檔案還原 🌕資料損毀，且資料無法復原 🌕資料損毀，僅可復原部分資料\_\_\_\_%〉* 遺失設備存放資料性質說明

〈個人敏感性資料、機密性資料、非機敏性資料，請說明內容〉\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 影響評估補充說明

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)* 毀損資料/系統已恢復正常運作
* 完成系統復原測試
* 通知事件相關當事人，並依內部資安通報作業向上級呈報【**如遺失設備存有敏感資料，此選項為必填**】
* 應變措施補充說明【請填寫補充說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎應變處置綜整說明【請說明損害控制或復原之執行狀況】： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 是否已完成損害控制或復原 🌕否，尚未完成損害控制或復原 🌕是，已完成損害控制 🌕是，已完成損害控制並復原 完成損害控制或復原時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |

|  |
| --- |
| **【參、調查、處理及改善報告-設備問題】(結報階段)** |
| **Step6.資安事件結案作業-設備問題**(請回傳P2-P4、P16-P18) |
| 六、事件調查與處理：◎受害資訊設備數量：電腦總計\_\_\_\_\_\_\_臺；伺服器總計\_\_\_\_\_\_\_臺； 其他設備\_\_\_\_\_\_\_ 總計\_\_\_\_\_\_\_\_臺 ◎IP位址(IP Address)(無；可免填)外部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 內部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎網際網路位址（Web-URL）(無；可免填)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎作業系統名稱、版本：🌕Windows系列 🌕Linux系列 🌕其他作業平台 版本：\_\_\_\_\_\_\_\_\_\_\_\_ ◎受害系統是否通過資安管理認證(ISMS)：🌕是 🌕否◎資安監控中心(SOC)：🌕無 🌕機關自行建置  🌕委外建置，該廠商名稱 ◎受害主機是否納入SOC監控範圍：🌕是 🌕否◎機關是否裝置資安防護設備：🌕是 🌕否(不須填寫資安防護類型) 資安防護類型〈複選〉〈□防毒軟體，監控設備代號：  □網路防火牆，監控設備代號：  □電子郵件過濾機制，監控設備代號：  □入侵偵測及防禦機制，監控設備代號：  □應用程式防火牆，監控設備代號：  □進階持續性威脅攻擊防禦措施，監控設備代號：  □其他，監控設備代號： 〉◎SOC業者是否發送事件告警資訊：🌕是 🌕否(不須填寫情資分析單編號) 情資單分析編號： ◎事件發生原因〈單選〉〈🌕設定錯誤 🌕設備異常/毀損 🌕電力供應異常 🌕人為疏失 🌕廠商維護環境或管理疏失 🌕無法確認事件原因《🌕無相關紀錄檢視 🌕相關紀錄遭異常刪除/變更🌕受限於資安人力/預算無法調查🌕逕行重 建無法調查🌕系統汰換逕行下架🌕事件調查後仍無法確認原因》🌕其他\_\_\_\_\_\_\_\_\_〉 【請說明事件調查情況】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎補強措施〈複選〉1. 補強系統/程式安全設定
	* + - * 檢視資訊設備使用年限
2. 資安管理與教育訓練〈複選〉
	* + - * 重新檢視機關網路架構適切性
				* 機關內部全面性安全檢測
				* 加強內部同仁資安教育訓練
				* 修正內部資安防護計畫

◎其他相關安全處置【請填寫相關處置、預定完成時程及成效追蹤機制】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎調查、處理及改善報告繳交(登錄結報)時間：\_\_\_\_\_\_\_年\_\_\_\_\_\_\_月\_\_\_\_\_\_日\_\_\_\_\_\_時\_\_\_\_\_\_分 |
| **【貳、損害控制或復原-其他】(應變處置階段)** |
| **Step5.請填寫機關緊急應變措施-其他**(請回傳P2-P4、P19-P20) |
| ◎保留受害期間之相關設備紀錄資料〈複選〉(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處罝說明」欄位說明)* 已保存遭入侵主機事件檢視器〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存防火牆紀錄〈單選〉

〈🌕1個月 🌕1-6個月 🌕6個月以上 🌕其他\_\_\_\_\_〉* 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共\_\_\_\_個
* 其他保留資料或資料處罝說明【如未保存資料亦請說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎事件分析與影響評估〈複選〉(最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明)經分析已保存之紀錄，是否發現下列異常情形：* 異常連線行為【請列出異常IP與異常連線原因，如：存取後台管理頁面】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 異常帳號使用【請列出帳號並說明帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 發現資料外洩情況【如：異常打包資料，請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 影響評估補充說明【請填寫補充說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎封鎖、根除及復原〈複選〉(最少選填一項，如無對應變處理方式，請於「應變措施補充說明」欄位說明)* 移除未授權存在之惡意網頁/留言/檔案/程式，共\_\_\_\_筆**(必填)**

【請說明程式名稱或路徑、檔名，如無須移除，請填寫「無」】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 將可疑IP/Domain Name列入阻擋清單**(必填)**【請說明設定阻擋之資訊設備與阻擋之IP，如無須阻擋，請填寫「無」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 停用/刪除異常帳號**(必填)**【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* 暫時中斷受害主機網路連線行為至主機無安全性疑慮
* 重新建置作業系統與作業環境，完成日期\_\_\_\_\_\_\_\_\_\_\_\_
* 惡意程式樣本送交防毒軟體廠商，共\_\_個
* 應變措施補充說明【請填寫補充說明】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎應變處置綜整說明【請說明損害控制或復原之執行狀況】： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  是否已完成損害控制或復原 🌕否，尚未完成損害控制或復原 🌕是，已完成損害控制 🌕是，已完成損害控制並復原  完成損害控制或復原時間：\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_日\_\_\_\_時\_\_\_\_分 |

|  |
| --- |
| **【參、調查、處理及改善報告-其他】(結報階段)** |
| **Step6.資安事件結案作業-其他**(請回傳P2-P4、P19-P22) |
| 六、事件調查與處理： ◎受害資訊設備數量：電腦總計\_\_\_\_\_\_\_臺；伺服器總計\_\_\_\_\_\_\_臺； 其他設備\_\_\_\_\_\_\_ 總計\_\_\_\_\_\_\_臺 ◎IP位址(IP Address)(無；可免填)外部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 內部IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎網際網路位址（Web-URL）(無；可免填)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎作業系統名稱、版本：🌕Windows系列 🌕Linux系列 🌕其他作業平台 版本：\_\_\_\_\_\_\_\_\_\_\_\_ ◎受害系統是否通過資安管理認證(ISMS)：🌕是 🌕否◎資安監控中心(SOC)：🌕無 🌕機關自行建置  🌕委外建置，該廠商名稱 ◎受害主機是否納入SOC監控範圍：🌕是 🌕否◎機關是否裝置資安防護設備：🌕是 🌕否(不須填寫資安防護類型) 資安防護類型〈複選〉〈□防毒軟體，監控設備代號：  □網路防火牆，監控設備代號：  □電子郵件過濾機制，監控設備代號：  □入侵偵測及防禦機制，監控設備代號：  □應用程式防火牆，監控設備代號：  □進階持續性威脅攻擊防禦措施，監控設備代號：  □其他，監控設備代號： 〉◎SOC業者是否發送事件告警資訊：🌕是 🌕否(不須填寫情資分析單編號) 情資單分析編號： ◎事件發生原因〈單選〉〈🌕社交工程 🌕作業系統漏洞 🌕弱密碼 🌕應用程式漏洞 🌕網站設計不當 🌕人為疏失 🌕設定錯誤 🌕設備異常/毀損 🌕電力供應異常 🌕廠商維護環境或管理疏失 🌕無法確認事件原因《🌕 無相關紀錄檢視🌕相關紀錄遭異常刪除/變更🌕受限於資安人力/預算無 法調查🌕逕行重建無法調查🌕系統汰換逕行下架🌕事件調查後仍無法 確認原因》🌕其他\_\_\_\_\_\_\_\_\_〉【請說明事件調查情況】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_◎補強措施〈複選〉1. 補強系統/程式安全設定〈複選〉
	* + - * 已完成評估變更透過受害主機登入應用系統密碼之必要性(如：使用受害主機登入之網域帳號密碼、公務系統帳號密碼、郵件帳號密碼等) **(必填)**
				* 已完成評估變更受害主機中所有帳號密碼之必要性(含本機管理者) **(必填)**
				* 已完成檢視/更新受害主機系統與所有應用程式至最新版本(包含網站編輯管理程式，如：FrontPage) **(必填)**【請說明主要更新之程式名稱，如無須更新，請填寫「皆已更新至最新版本」】

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* + - * + 關閉網路芳鄰功能
1. 資安管理與教育訓練(複選)
	* + - * 重新檢視機關網路架構適切性
				* 機關內部全面性安全檢測
				* 加強內部同仁資安教育訓練
				* 修正內部資安防護計畫

◎其他相關安全處置【請填寫相關處置、預定完成時程及成效追蹤機制】\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ◎調查、處理及改善報告繳交(登錄結報)時間：\_\_\_\_\_\_\_年\_\_\_\_\_\_\_月\_\_\_\_\_\_日\_\_\_\_\_\_時\_\_\_\_\_\_分 |

# 附件4：變更申請單

|  |
| --- |
| **步驟一：變更申請　　(申請日期：　　年　　月　　日)** |
| 維運廠商 |  | 維運人員 |  |
| 資通系統/設備名稱 |  |
| 預計執行日期時間 | 年 月 日 時 分 |
| 預計完成日期時間 | 年 月 日 時 分 |
| 變更分類(可複選) | □程式異動 (如為應用系統變更，請完成「附件、系統更版上線前檢核表」)□作業系統弱點修補□作業系統升級 □資料庫 □套裝軟體 □安全組態(例如:GCB) □網路架構/網路設備 □硬體□各類設備之設定檔異動(不包含防火牆政策)□虛擬主機變更□其他  |
| 變更需求描述 |  |
| 影響範圍 | （資訊資產、資訊系統服務或資訊作業流程）： |
| 服務潛在風險或衝擊 | □高(服務中斷12小時以上)□中(服務中斷12小時以內)□低(服務不中斷)其他補充： |
| 變更文件審查 | □變更回復計畫 □測試報告 □其他：□程式源碼檢測報告 |
| 測試結果 | □通過 □不通過(請填寫說明)  |
| 程式源碼檢測 | □人工檢視，並檢附修正前後版本差異程式源碼。□工具檢測 檢測人員簽核：＿＿＿＿＿＿＿＿＿＿ |
| 承辦人 | 科長 |
|  |  |
| **步驟二：執行變更** |
| 變更日期 |  |
| 驗收標準 |  |
| 變更結果 | □成功□失敗，原因說明： |
| 承辦人 |  | 日期 |  |
| 承辦科科長 |  | 日期 |  |

|  |
| --- |
| **附件、系統更版上線前檢核表** |
| 安裝環境（OS） | □Windows系列 □CentOS □Unix系列 □其他＿＿＿＿＿ |
| 檢核人員(系統負責人) |  |
| 檢核項目 | 評估適用項目 | 備註 |
| 資通系統 |
| 完整性 | 已評估風險及識別可能之威脅（如OWASP Top 10），且修正需求內容或採取補償性控制措施，並提供佐證紀錄或報告。 | □是□否□不適用 |  |
| 上版前已留有測試紀錄。 | □是□否□不適用 |  |
| 其他：請依各系統需求新增 | □是□否□不適用 |  |
| 機密性 | 以最小權限存取設計用戶可存取之資訊範圍，以最少欄位資訊顯示為原則。 | □是□否□不適用 |  |
| 依不同角色身分給予存取權限，確保權責分離。 | □是□否□不適用 |  |
| 應採用加密技術儲存含有機敏資料於資料庫或檔案中。 | □是□否□不適用 |  |
| 對於儲存於檔案、資料庫之資訊，如有個人資料(例如：密碼、身份證字號、住家地址…等)制定必要的控管措施與加密儲存及傳輸，並留存使用紀錄。 | □是□否□不適用 |  |
| 可用性 | 系統版更前已擬訂版更失敗之緊急復原計畫程序。 | □是□否□不適用 |  |
| 系統版更後已同步更新相關操作手冊。 | □是□否□不適用 |  |
| 作業環境安全檢查 | 作業系統已更新至最新版本（若無法更新至最新版本請述明原因）。 | □是□否□不適用 |  |
| 如為對外服務之應用系統，系統版更後是否使用Qualys SSL Labs 檢查，確保通訊協定相關弱點已修補完成。<https://www.ssllabs.com/index.html> | □是□否□不適用 |  |

# 附件5：經費估算表

|  |
| --- |
| **花東基金補助計畫管理資訊系統改版建置委外服務案經費估算表** |
| 項次 | 項目 | 估算方式 | 單價 | 數量 | 單位 | 預估金額(元) |
| 1 | 花東基金補助計畫管理資訊系統建置 | 　 | 　 | 　 | 人月 |  |
| 2 | 跨系統資料介接 | 　 | 　 | 　 | 人月 |  |
| 3 | 駐點人員 |  |  |  | 人月 |  |
| 4 | 客服專線諮詢服務 | 　 | 　 | 　 | 人月 |  |
| 5 | 資通安全管理及維護 | 　 | 　 | 　 | 人月 |  |
| 6 | 教育訓練 |  |  |  | 場次 |  |
| 7 | 專案管理 | 　 | 　 | 　 | 人月 |  |
| **總 計（中文大寫，含稅後價格)** |  |