國家發展委員會

「花東基金補助計畫管理資訊系統維運及功能擴充 109 年至 110 年委外服務案」

（案號：ndc109053）

需求說明書

中華民國 109 年 7 月

目次

壹、專案說明

一、專案名稱

花東基金補助計畫管理資訊系統維運及功能擴充 109 年至 110 年委外服務案(以下簡稱本專案）。

二、背景說明

（一）專案緣起

為協助花東地區發展，並使其擁有與西部均等的發展機會，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)，使花東地區永續發展有了法源依據及基金預算，基金總額新臺幣(以下同)400 億元，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，迄今業推動第 3 期，為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，爰本會於 108 年 10 月委外建置花東基金補助計畫管理資訊系統。

為強化花東基金補助計畫系統管考功能、相關表報分析及計畫空間管理資訊，擬新增系統部分功能，使系統運作更加順暢，爰規劃「花東基金補助計畫管理資訊系統維運及功能擴充 109 年至 110 年委外服務案」。

（二）使用對象

1、中央政府：花東基金補助計畫之中央主管部會(含行政院及中央部會)。

2、縣政府：花蓮縣政府及臺東縣政府(含鄉鎮市公所)。

3、本會。

（三）設備說明

1.花東基金補助計畫管理資訊系統目前設備位於行政院所屬委員會雲端資料中心。網址為 http://117.56.91.109/NDCPMIS/CMBASE/Main.aspx

2.本網站前後臺架設在雲端中心虛擬主機，為專案型規格 (4 顆 vCPU、8GB 記憶體、100GB 硬碟)，說明如下：

項目	系統名稱	規格配備	備註
1	Microsoft Windows 2016 server	網頁伺服器	網站伺服器軟體：IIS10.0
2	Microsoft SQL Server 2019	資料庫伺服器	

三、專案目標

（一）強化及維護本系統功能正常運作。

（二）配合行政院花東基金補助計畫管理需求，進行系統各項功能增修。

（三）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

專案範圍包括本系統之維運、功能增修及資訊安全等。

五、專案期程

本專案期程為自決標次日起至 110 年 12 月 31 日止。

六、專案預算

本專案預算為新臺幣（以下同）150 萬元整。

貳、需求說明

一、功能維護及客服

(一)為提升花東基金補助計畫管理效率，本專案應提供維持本系統各項功能及資料匯入系統平臺正常運作之相關服務。遇有系統運作障礙，得標廠商應於接獲本會通知（電話、Email、傳真或書面等方式）後，4 個小時內回應本會，回應內容應至少包含預計處理方式、預估工作人日及預計完成日期，經本會確認後，於期限內完成該項需求功能調整、維護等相關作業，並確實記錄處理狀況。

(二)廠商須配合本會正常上班時間，提供系統諮詢專線及服務，服務範圍包含使用者以電話、email 或線上反應之各項系統操作使用、疑難排解等問題或諮詢，並彙集相關記錄於維護報告內。

(三)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)其他維運調整作業：根據使用者提出之問題，以不更動原作業流程狀態下，調整原功能或報表。其項目包含 1.系統內經常性之報表、流程調校。2.資料處理計算規則、檢核方式及資料篩選條件之調整。3.因應使用者需求，提供資料輸出以開放資料形式轉出之功能，與使用者進行需求訪談後確認。4.協助使用者新增帳號等作業。

二、功能增修

(一)配合行政院花東基金補助計畫管理需求，提供以部會別、計畫別、需求時間別等所需之系統資料輸出功能，相關報表格式須與使用者進行需求確認後開發設計。

(二)優化目前各角色使用介面及提升彈性報表產出之便利性，並依據管理需求，建置綜合查詢介面，提供計畫分年及全期各

項執行資訊。

(三)針對主辦機關與督導部會等不同角色於系統進行填寫與審查之歷程予以紀錄，並以適當方式於使用介面呈現填審及資料修改歷程，以提升計畫管理效能。

(四)運用「個案計畫空間管理資訊系統」建立計畫地理空間資料。建立與「個案計畫空間管理資訊系統」之空間資料填報及資料串接介面，並協助花東兩縣政府補實相關資訊，以提升空間資訊之正確性。

(五)開發儀表板圖表分析功能，提供表報產製及系統預警功能，落實部會督導、協助機制，提升決策支援性。

(六)其它功能增修：於本專案契約期程內，應依據本會需求，由本會與廠商於專案會議進行討論，並依專案會議之會議決議進行。

三、教育訓練

辦理 2 場次系統教育訓練：

(一)訓練課程、場次及時間由本會指定，授課人員及其資格應先經本會同意。

(二)授課時數以 3 小時為原則，教育訓練人數約為 30 至 50 人，得標廠商須提供每場次受訓學員所需教材及學員餐飲。

(三)教育訓練成果報告至少包含：課程資料(主題、日期及地點)、上課人員簽到表(得由本會提供)、佐證相片及課程講義等內容。

(四)外聘講師鐘點費、車馬費、食宿費、教材編印費、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。

四、辦理期程

辦理期程	工作內容
決標次日起 20 日內	專案工作計畫書(內容至少包含專案組織、人員分工職掌、專案管理機制、資通安全與保密計畫、資通系統防護基準之控制措施項目及工作項目細部時程規劃等)。
決標次日起 2 個月內	1. 完成依部會別產出之管考報表及報告。 2. 完成依計畫別產出個別計畫之報表。 3. 完成以季為單位產出之報表。 4. 完成管考專用報表。 5. 完成綜合查詢介面建置，並提供系統功能新增調整測試報告。
109 年 11 月底前	1. 完成維運報告(期間自決標次日起至 109 年 11 月 20 日)。 2. 資安防護基準之控制措施與 GCB 之執行進度報告
110 年 2 月底前	1. 完成主辦機關與主管部會於系統進行填寫與審查之歷程紀錄。 2. 提供使用者介面可呈現填審及資料修改歷程之功能(如已填報、已審查)。 3. 建立與「個案計畫空間管理資訊系統」之空間資料填報及資料串接介面，使用介面呈現填審及資料修改歷程之功能，並協助花東兩縣政府補實相關資訊。 4. 資安防護基準之控制措施與 GCB 之執行進度報告。
110 年 7 月底前	1. 完成各角色使用者介面優化及彈性報表介面，並提供系統功能新增調整測試報告。 2. 提供計畫分年及全期各項執行資訊。 3. 資安防護基準之控制措施與 GCB 之執行進度報告。

辦理期程	工作內容
110 年 8 月 10 日前	維運報告(期間自 109 年 11 月 21 日起至 110 年 7 月 31 日)。
110 年 8 月底前	完成教育訓練。
110 年 10 月底前	1. 完成儀表板圖表分析功能。 2. 提供表報產製及系統預警功能。
110 年 12 月 10 日前	1. 維運報告(期間自 110 年 8 月 1 日起至 110 年 11 月 30 日)。 2. 專案結案報告書及系統原始程式碼及資料備份(以電子檔方式交付)。 3. 系統測試報告(測試計畫說明、測試項目清單、各系統功能逐項測試報告、測試人員簽章)。 4. 系統維護手冊(系統環境及架構、軟硬體需求、系統維護說明、資料庫維護說明)。 5. 系統復原演練報告。 6. 結案報告(含維運報告、系統操作手冊、各功能測試報告、客服服務工作報告、資安防護基準自評表、災難復原計畫與報告及教育訓練成果報告等)。

參、專案管理需求

一、專案工作小組

本案廠商應成立專案工作小組，負責本案各項需求規劃、協調、分析、程式系統開發、設計、測試及維護管理等工作，並應於執行期間依管控進度製作紀錄,以備專案執行過程中進行查核。

(一)人員管理

1. 廠商於專案管理計畫書中所列之本專案全部工作項目及人員。
2. 專案成員資料，應提供學經歷、專長、本案代理人、

本案負責之工作項目與內容。

3. 廠商應於第一次專案協商並確認專案執行工作之人力安排、作業規劃及雙方配合事項，並指定專人負責協調聯繫等相關事宜。
4. 廠商如需更換應先提出書面簡歷資料，徵得本會審閱及同意後，才可以正式替換接任。
5. 如因人員不適任致本專案工作進度落後，本會有權要求更換並增加工作人員以完成本專案相關工作，承商不得要求增加費用。
6. 專案負責人及專案經理必須為承商在職員工。

(二)專案會議

為落實專案的執行與推動，承商應配合召開專案會議，報告專案執行進度及問題列管追蹤。

二、專案控管方式

(一)廠商應於規定期限提交工作計畫書，工作計畫書內容須詳述含專案管理計畫、專案執行方法、各工作項目之執行方式、工作時程、開發工具、資料建置、管理技術、人力資源、時程控管、專業諮詢、系統功能測試計畫、支援服務及交付驗收項目等。

(二)廠商於應用系統規劃分析、開發設計前，應先訪談作業單位確認其功能需求，經本會審查同意後，始得據以進行；進行期間如有變更之必要，應經本會同意。

(三)本案規劃分析成果及系統內容，廠商應負保密義務，非經本會書面同意，不得以任何形式部分或全部對外發表。

(四)於本案執行期間，本會禁止使用非本會許可設備，進行遠端遙控方式管理主機及更新程式、資料，系統規劃建置事宜，系統建置需遵守本會資訊安全規定及相關措施，如有違反，依契約書規定辦理。

(五)各工作項目完成、系統操作或辦理內容有所爭議或有重要事項需協調時，本會得召開專案會議進行研議，俾利檢討及解決問題，廠商專案負責人及指定人員應配合出席；廠商須於專案會議中，就最新專案執行成果、情形及交付文件提出報告。

(六)雙方得視需要不定期召開工作會議，由雙方共同議定會議日期，廠商須報告本案工作相關進度。

肆、雙方責任

一、本會責任

(一)參與本案各工作項目之會議。

(二)配合提供相關資料並參與規劃過程。

二、廠商責任

(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。

(二)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。

伍、交付項目

一、交付項目及期程

承商應配合各階段工作時程提交相關文件予本會，各階段交付文件，除另有規定外，應交付紙本 1 式 2 份，以 A4 尺寸紙張製作及裝訂，封面應註明本會名稱、本案名稱、交付文件名稱及承商名稱，前開文件應附加電子檔且燒錄成光碟 1 式 1 份。相關文件撰寫如有疑義，應提報專案會議確認，以為後續處理之依據。

本案分 3 期撥款，各期應交付之細部項目及時程由廠商依據各期查核點規定時間及項目規劃，並經本會同意後依進度執行。

各期交付項目及時程規劃如下，交付期限如遇假日，則順延至下一個工作天。

各期交付項目及時程

期別	交付項目	交付時間
第 1 期	1. 專案工作計畫書(內容至少包含專案組織、人員分工職掌、專案管理機制、資通安全與保密計畫、資通系統防護基準之控制措施項目及工作項目細部時程規劃等)。	決標次日起 20 日內
	2. 完成各項依部會別、計畫別及需求時間別等所需之系統資料報表輸出功能。 3. 完成管考專用報表。 4. 完成綜合查詢介面建置，並提供系統功能新增調整測試報告。	決標次日起 2 個月內
	5. 維運報告：期間自決標次日起至 109 年 11 月 20 日。 6. 資安防護基準之控制措施與GCB之執行進度報告。	109 年 11 月底前
第 2 期	1. 完成主辦機關與主管部會於系統進行填寫與審查之歷程紀錄。 2. 提供使用者介面可呈現填審及資料修改歷程之功能(如已填報、已審查)。 3. 建立與「個案計畫空間管理資訊系統」之空間資料填報及資料串接介面，使用介面呈現填審及資料修改歷程之功能，並協助花東兩縣政府補實相關資訊。 4. 資安防護基準之控制措施與GCB之執行進度報告。	110 年 2 月底前
	5. 完成各角色使用介面優化及彈性報表介面，並提供系統功能新增調整測試報告。 6. 提供計畫分年及全期各項執行資訊。 7. 資安防護基準之控制措施與GCB之執行進度報告。	110 年 7 月底前
	8. 維運報告：期間自 109 年 11 月 21 日起至 110 年 7 月 31 日。	110 年 8 月 10 日前
第 3 期	1. 完成教育訓練。	110 年 8 月底前

期別	交付項目	交付時間
	2. 完成儀表板圖表分析功能。 3. 提供表報產製及系統預警功能。	110 年 10 月底前
	4. 維運報告：期間自 110 年 8 月 1 日起至 110 年 11 月 30 日。 5. 專案結案報告書及系統原始程式碼及資料備份(以電子檔方式交付)。 6. 系統測試報告(測試計畫說明、測試項目清單、各系統功能逐項測試報告、測試人員簽章)。 7. 系統維護手冊(系統環境及架構、軟硬體需求、系統維護說明、資料庫維護說明)。 8. 系統復原演練報告。 9. 結案報告(含維運報告、系統操作手冊、各功能測試報告、客服服務工作報告、資通系統防護基準自評表、災難復原計畫與報告及教育訓練成果報告等)。	110 年 12 月 10 日前

二、查驗與驗收

(一)各期工作項目必須依上述時程交付。

(二)廠商應於各階段查驗或驗收時，完成交付查驗或驗收確認單和應交付文件項目，來函本會辦理驗收事宜。

(三)交付內容查驗或結案驗收時，如發現不符本案規格或需求者，除另有規定外，承商應於 10 個工作天內完成修正，並通知本會安排複查或複驗，以完成查驗或驗收程序。

(四)各期交付項目須經本會審核同意後方視為合於查驗或驗收標準。

(五)維運部分須符合本專案服務水準。

陸、資訊安全規範

一、廠商於原契約有效期間內及期滿或終止後，對於所得知或持有

本會之公務機密,均應以善良管理人之注意妥為保管及確保其機密性,並限於本契約目的範圍內,於機關指定之處所內使用之。非經本會事前書面同意,廠商不得為本人或任何第三人複製、保有、利用該等公務秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等公務機密,或對外發表或出售,亦不得攜至機關或機關所指定處所以外之處所。

二、本系統資通安全等級為中級,得標廠商需完成相關防護基準之控制措施(詳如行政院資通安全會報網站/資安法專區/資通安全責任等級分級辦法-附表十資通系統防護基準(如附件1);資通系統防護基準自評表(如附件2)。

三、人力資源安全

(一)人員若接觸本會資訊,應簽署「保密切結書」與「保密同意書」,使其瞭解未遵循資訊安全相關規定,或行使任何危及本會資訊安全之行為,將依相關法規辦理,或訴諸適當之懲罰與法律行動。

(二)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:資訊或資訊安全相關證照)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。

四、通訊與作業安全管理

(一)作業系統須使用防毒軟體或採用其他防護設備,並即時更新病毒碼,且定期對電腦系統及資料儲存媒體進行病毒掃描。

(二)作業系統上的程式和軟體,必須測試成功後才能部署,除功能測試外,亦應執行相關安全性檢視(如:弱點掃瞄、病毒檢測、程式原始碼檢視等),以及評估對其他系統的影響。

(三)配合本會弱點掃描(包含主機與網站)與滲透測試作業,屬於「高風險」之弱點應依據弱掃報告或滲透測試報告,匯整於「ISMS-B.07-03弱點處理報告表」(附件3)於規定期限內改善完成。

五、系統獲取、開發及維護

(一)系統測試時或安裝前應進行檢查，應包含但不限於弱點掃描、滲透測試、程式原始碼掃描等，並提供相關報告或紀錄。廠商提供之系統若發現資訊安全漏洞時，須主動或配合進行修正作業。

(二)各項軟硬體設備安裝時，其作業系統與相關軟體之修補程式應更新至最新版，如有例外狀況應經本會核准。

(三)應定期確認系統軟體版本，對作業系統及應用系統進行任何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。

(四)廠商對於重大資訊安全威脅發生時應主動提供維護服務，並配合本會處理與通報資通安全事件的責任與作業程序。

(五)具即時安全防護措施及監測機制，當網站發生資安事故或偵測到任何未經授權之網頁內容變更等異常現象時，需即時通報相關人員，同時自動回復為原始網頁內容；事後並針對事故說明發生原因及提出檢討報告。

(六)維護標的如發生資通安全事件時，應第一時間通報本會承辦人員，並配合本會進行資通安全事件處理及1小時內填具「資通安全事件通報單」，並依資通安全事件等級(第一級或第二級七十二小時內，第三級或第四級三十六小時內)完成損害控制或復原作業，一個月內送交資通安全事件調查、處理及改善報告(附件4)。

(七)遠端系統建置及維護工作，應規劃詳細標準作業程序（含人員、IP及帳號控管等），以及如何防止非法入侵之處理方式。

六、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，廠商接獲通知後應配合執行。

七、廠商執行專案過程中，如有部份工作項目分包給其他供應者執行，應主動知會本會相關權責人員，並取得書面同意之核准紀錄。如有分包之情形，廠商應要求分包商遵循本會資訊安全管理制度相關規範。

八、應用系統

(一)網站應以HTTPS安全通訊協議(SSL加密、認證機制)進行網頁開發，以加強網路應用的安全性。

(二)應用系統開發須避免資訊安全組織公布已知易遭駭客攻擊之弱點，如OWASP(Open Web Application Security Project)組織公布之10大關鍵網站應用程式風險(Top 10 Most Critical Web Application Security Risks)，及未來發布之安全問題種類。

(三) 廠商因本案所交付或提供本會利用之系統，應有一定異常偵測機制，以確保資料機敏性與完整性，並於異常存取或變更情形發生時，應可自動通知廠商及本會。

九、系統與資料庫備份

系統與資料庫備份除一般備份與回復(Backup & Restore)的標準程序之外，應包含以下的作業：

1. 進行備份自動化管理與排程。
2. 可在不中斷服務情形下進行檔案系統及資料庫線上備份。
3. 系統備援。

十、系統轉移

為利系統後續委商之營運，本案廠商須交付「移轉標準化作業程序書」，並配合下列事項：

1. 實際交接移轉：自新承接廠商決標日起，應無償提供2個人月的實際移轉交接作業，包含相關技術支援及諮詢等服務，輔導新承接廠商營運事宜，應於本會提出移轉交接需求時，擬具作業計畫，經本會同意後據以執行。與新廠商交接移轉期間，本案各項服務不得中斷並持續提供至新承接廠商完成全案建置及移轉作業。
2. 如承接廠商為本案廠商，則不需進行實質移轉，但仍須交付「移轉標準化作業程序書」，以達本系統持續營運及系統服務未來平順移轉之目的。

十一、廠商於維運期間配合本會資訊安全或系統升級等需求衍生之軟硬授權，不得請求額外費用，以符合資料安全基本原則；如系統發生足以影響資料安全之程式漏洞，應即時無條件配合修改所開發之程式。

柒、其他事項

一、本會如有導入虛擬化作業，廠商應配合本案系統虛擬化轉移，若須修正程式需求，廠商亦應配合修改。

二、花東縣政府有關系統資料介接、匯入等需求，請提供技術諮詢與協助。

三、本案開發之系統、報表財產歸屬均屬本會所有。

四、本文件於決標後納入契約附件。

五、有關本案所作之各項內容，其著作權及智慧財產權悉歸本會所有。任何本案所完成或未完成之相關創作及技術資料，廠商均有保密義務，且非經本會書面同意，均不得任意移轉或交付任何第三人。

六、其他未盡事宜，依據「政府採購法」及其相關規定辦理。

捌、服務建議書格式

一、以中文由左至右（直式橫書）擅打，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 11 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：

一、執行能力及履約能力(含廠商規模及承製相關專案之實績等)

二、技術建議

三、專案工作規劃與管理

四、創新與加值服務

五、價格之完整性與合理性（需詳列報價內容，請依照經費估算表(附件 5)填列）

六、廠商企業社會責任(CSR)指標（後續履約期間給予全職從事本採購案之員工薪資至少新臺幣 3 萬元以上）

七、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

玖、附件

附件 1、資通系統防護基準

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。
稽核與可歸責性	稽核事件	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。		一、依規定時間週期及紀錄留存政策，保留稽核紀錄。 二、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。 三、應稽核資通系統管理者帳號所執行之各項功能。
	稽核紀錄內容	一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二、等級「普」之所有控制措施。		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，確保輸出格式之一致性。
	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。		
	稽核處理失效之回應	一、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。 二、等級「中」及「普」之所有控制措施。	資通系統於稽核處理失效時，應採取適當之行動。	
	時戳及校時	一、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。 二、等級「普」之所有控制措施。		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)。
	稽核資訊之保護	一、定期備份稽核紀錄至與原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對稽核紀錄之存取管理，僅限於有權限之使用者。
營運持續計畫	系統備份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、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。 三、等級「中」之所有控制措施。	一、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。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。
	系統備援	一、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。 二、原服務中斷時，於可容忍時間內，由備援設備取代提供服務。		無要求。
識別與鑑別	內部使用者之識別與鑑別	一、對帳號之網路或本機存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	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。	

	身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三、等級「普」之所有控制措施。	一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、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。 四、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。 五、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	
	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。	無要求。
	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)。	
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。	
	系統發展生命週期設計階段	一、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。 二、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。	無要求。
	系統發展生命	一、執行「源碼掃描」安全檢測。	一、應針對安全需求實作必要控制措施。

	週期開發階段	二、具備系統嚴重錯誤之通知機制。 三、等級「中」及「普」之所有控制措施。	二、應注意避免軟體常見漏洞及實作必要控制措施。 三、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。	
	系統發展生命週期測試階段	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署與維運階段	一、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。 二、等級「普」之所有控制措施。		一、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。 二、資通系統相關軟體，不使用預設密碼。
	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、可用性、完整性）納入委外契約。		
	獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
	系統文件	應儲存與管理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	一、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。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大長度金鑰。 四、加密金鑰或憑證週期性更換。 五、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。	無要求。	無要求。

	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。	無要求。	無要求。
系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
	資通系統監控	一、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。 二、等級「中」之所有控制措施。	一、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。 二、等級「普」之所有控制措施。	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、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。	無要求。

備註：

一、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。

二、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之系統防護基準。

附件2

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
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	

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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	

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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	

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	
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	
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	
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	
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	
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	

附件 3：ISMS-B.07-03 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	

附件4：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（http://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 P25-P27
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 P25-P29、非法入侵 P25-P27，P32-P33、阻斷服務 P25-P27，P35、設備異常 P25-P27，P37、其他 P25-P27，P39-P41）
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 P25-P31、非法入侵 P25-P27，P32-P34、阻斷服務 P25-P27，P35-P36、設備異常 P25-P27，P37-P38、其他 P25-P27，P39-P41）

【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

◎資安監控中心(SOC)：□無 □機關自行建置

□委外建置，該廠商名稱_____

◎資安維護廠商：_____

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P25-P29)

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置說明」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月以上 □其他 〉

□ 已保存防火牆紀錄〈單選〉

〈□1 個月 □1 - 6 個月 □6月以上 □其他 〉

□ 已保存網站日誌檔〈單選〉

〈□1 個月 □1 - 6 個月 □6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置說明【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】:
_____
_____
_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

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P25-P31)

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

◎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：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎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□系統遭入侵□其他_____ 〉

◎請簡述事件處理情況：_____

_____

_____

◎補強措施〈複選〉

I. 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)

II. 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 P25-P27、P32-P33)

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置說明」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月以上 □其他 〉

□ 已保存防火牆紀錄〈單選〉

〈□1 個月 □1 - 6 個月 □6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置說明【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

□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】:

_____

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

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 P25-P27、P33-35)

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

◎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：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎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

□系統遭入侵□其他 _____〉【請說明事件調查情況】

_____

_____

◎補強措施〈複選〉

I. 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

II. 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 P25-P27、P34-P35)

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置說明」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月以上　☐其他　〉

☐已保存防火牆紀錄〈單選〉

〈☐1 個月　☐1 - 6 個月　☐6月以上　☐其他　〉

☐已保存受攻擊主機封包紀錄(☐10 分鐘☐ 0-30 分鐘☐ 30-60 分鐘〉

☐其他保留資料或資料處置說明【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】：

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

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 P25-P27、P35-36)

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

◎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：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎補強措施〈複選〉

I. 補強系統/程式安全設定〈複選〉

□限制同時間單一 IP 連線

□DNS 主機停用外部遞迴查詢

□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」】

_____

_____

□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」】

_____

_____

II. 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-設備異常】(應變處置階段)

Step5.請填寫機關緊急應變措施-設備異常(請回傳 P25-P27、P38-40)

◎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置說明【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】:

_____

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

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-設備異常】(結報階段)

Step6.資安事件結案作業-設備異常(請回傳 P25-P27、P36-P37)

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

◎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：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎事件發生原因〈單選〉

〈□設定錯誤□設備毀損□系統遭入侵□電力供應異常□人為疏失

□其他_____〉【請說明事件調查情況】

_____

_____

◎補強措施〈複選〉

I. 補強系統/程式安全設定

□檢視資訊設備使用年限

II. 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 P25-P27、P38-P41)

◎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置說明」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月以上　☐其他　〉

☐已保存防火牆紀錄〈單選〉

〈☐1 個月　☐1 - 6 個月　☐6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置說明【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】:

_____

_____

_____

○已完成損害控制，未有擴大損害情形

○已完成損害控制並復原，恢復資安事件造成的損害

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 P25-27、P38-40)

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

◎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：_____

◎已裝置之安全機制：

□防火牆 □防毒軟體 □入侵偵測系統 □入侵防禦系統 □其他：_____

◎受害系統是否通過資安管理認證(ISMS)：□是 □否

◎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□設備毀損

□系統遭入侵□電力供應異常□其他_____ 〉【請說明事件調查情況】

_____

◎補強措施〈複選〉

I. 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」】

_____

_____

☐關閉網路芳鄰功能

II. 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5

「花東基金補助計畫管理資訊系統維運及功能擴充109年至110年委外服務案」(案號：ndc109053)經費估算表

單位：元

項次	服務項目	估算方式	單價	數量	單位	預估金額
1	系統擴充管控整體規劃作業					
2	系統擴充功能需求					
3	配合本會軟硬體環境建置需求					
4	資訊管理維護及客服					
5	教育訓練					
總計新臺幣(中文大寫)：						