擬請公告周知。

檔　　號：
保存年限：

謝宜亨 108/12/1

如辦

行政院公共工程委員會　函

地址：11010 臺北市信義區松仁路3號9樓
聯絡方式：(承辦人)蔡先生
(聯絡電話)02-87897607
(傳真)02-87897674
(E-mail)thy1513@mail.pcc.gov.tw

受文者：如行文單位

發文日期：中華民國108年12月9日
發文字號：工程技字第1080201430號
速別：普通件
密等及解密條件或保密期限：
附件：行政院108年11月15日院授發檔(資)字第1080008553號函及其附件1份

主旨：函轉行政院修正「公文電子交換系統資訊安全管理規範」相關資料，請查照並請轉知所屬。

說明：依據行政院108年11月15日院授發檔(資)字第1080008553號函辦理(如附件)。

正本：各技師公會、各工程技術顧問同業公會(以電子交換或電子郵件寄送)
副本：

主任委員 吳澤成

檔　　號:
保存年限:

行政院 函

地址：10058 臺北市中正區忠孝東路一段1號
承辦人：陳嘉浩
電話：02-89953548
傳真：02-89956468
E-Mail：ch_chen@archives.gov.tw

受文者：行政院公共工程委員會

發文日期：中華民國108年11月15日
發文字號：院授發檔(資)字第1080008553號
速別：普通件
密等及解密條件或保密期限：
附件：修正總說明、修正對照表、附錄修正對照表、公文電子交換系統資訊安全管理規範（A00000000A_1080008553_doc1_Attach1.pdf、A00000000A_1080008553_doc1_Attach2.pdf、A00000000A_1080008553_doc1_Attach3.pdf、A00000000A_1080008553_doc1_Attach4.pdf）

主旨：修正「公文電子交換系統資訊安全管理規範」，自即日起生效，請查照並轉知所屬。

說明：檢送旨揭規範、修正總說明、修正對照表及附錄修正對照表各1份，前揭內容業登載於國家發展委員會檔案管理局全球資訊網（網址：https://www.archives.gov.tw）。

正本：總統府及其所屬、國家安全會議及其所屬、立法院秘書長、司法院秘書長及司法院所屬、考試院秘書長及考試院所屬、監察院秘書長及監察院所屬、行政院秘書長及行政院所屬部會行總處署、直轄市政府、縣(市)政府、直轄市議會、縣(市)議會
副本：行政院法規會、國家發展委員會法制協調中心(均含附件) 電子公文交換章 2019/11/18 08:19:42

行政院公共工程委員會
秘書處 1080029121

公文電子交換系統資訊安全管理規範修正總說明

為共同維護公文電子交換系統安全及順遂業務推動，公文電子交換系統資訊安全管理規範(以下簡稱本規範)前於一百零三年二月五日以院授發檔(資)字第一０三０００八０四三號函訂定施行，並於一百零五年四月二十九日進行第一次修正。

本次修正係基於資通安全管理法暨相關子法施行及實務推動經驗，並考量公文電子交換系統最新功能架構之安全防護需要，爰修正本規範，修正重點如下：

一、 新增資通安全管理法及相關子法為法令適用依據。(修正規定第二點)

二、 考量法人或非法人團體等非政府機關加入公文電子交換系統之運作，與政府機關往來密切，須斟酌國家整體資訊安全，增訂該等用戶為本規範適用對象。(修正規定第三點)

三、 依公文電子交換系統最新四層架構，增列機關層之定義及調整終端層等之定義說明。(修正規定第四點)

四、 整併原各層級安全規定事項，增列防毒作業、主機禁止安裝點對點(P2P)應用程式等軟體、系統資安事件通報、憑證效期維護及密碼模組使用等共通性安全事項；增修交換層機關提供網頁版公文收發模組管理規定、機關層系統更版作業、機關層主機專機專用等內容；刪除終端層機關連線異動申請表格式規定、終端層機關主機專機專用與採用固定 IP、終端層主機備份封存、終端層公文收發人員教育訓練及天元模組使用管理等內容。(修正規定第五點)

五、 最新公文電子交換系統架構已達虛擬集中化之最適經濟規模，爰刪除有關系統虛擬集中化相關規定。(修正規定第六點)

六、 因應系統防護需要，增列自管中心將日誌傳送管理層進行監控聯防規定。(修正規定第七點)

七、 依公文電子交換系統最新架構，新增交換層對所屬機關層辦理稽核作業規定。(修正規定第九點)

八、 為順遂管理層及交換層機關辦理中止機關(構)系統服務作業，增訂中止服務流程規定;因應管理實務需要，新增得中止機關(構)系統服務之違規情形及資通安全管理法主管機關通知發生重大危害資安事故之機關(構) 中止服務規定。(修正規定第十三點)

九、 配合第五點刪除天元模組使用管理及終端層機關連線異動申請表格式規定，刪除附錄一「公文 G2B2C 資訊服務中心連線異動申請表」、附錄二「天元模組遺失毀損報告單」、附錄三「天元模組緊急狀況處置報告單」;配合第九點增列交換層對所屬機關層辦理稽核作業需要，增列附錄二「公文電子交換系統(交換層對機關層)資訊安全稽核彙整表」; 配合第十三點增訂中止服務流程規定，增列附錄四「公文電子交換系統用戶中止服務流程」; 原附錄四及附錄五依序調整序號為附錄一及附錄三，並配合修正內容。

公文電子交換系統資訊安全管理規範修正總說明

為共同維護公文電子交換系統安全及順遂業務推動，公文電子交換系統資訊安全管理規範(以下簡稱本規範)前於一百零三年二月五日以院授發檔(資)字第一０三０００八０四三號函訂定施行，並於一百零五年四月二十九日進行第一次修正。

本次修正係基於資通安全管理法暨相關子法施行及實務推動經驗，並考量公文電子交換系統最新功能架構之安全防護需要，爰修正本規範，修正重點如下：

一、 新增資通安全管理法及相關子法為法令適用依據。(修正規定第二點)

二、 考量法人或非法人團體等非政府機關加入公文電子交換系統之運作，與政府機關往來密切，須斟酌國家整體資訊安全，增訂該等用戶為本規範適用對象。(修正規定第三點)

三、 依公文電子交換系統最新四層架構，增列機關層之定義及調整終端層等之定義說明。(修正規定第四點)

四、 整併原各層級安全規定事項，增列防毒作業、主機禁止安裝點對點(P2P)應用程式等軟體、系統資安事件通報、憑證效期維護及密碼模組使用等共通性安全事項；增修交換層機關提供網頁版公文收發模組管理規定、機關層系統更版作業、機關層主機專機專用等內容；刪除終端層機關連線異動申請表格式規定、終端層機關主機專機專用與採用固定 IP、終端層主機備份封存、終端層公文收發人員教育訓練及天元模組使用管理等內容。(修正規定第五點)

五、 最新公文電子交換系統架構已達虛擬集中化之最適經濟規模，爰刪除有關系統虛擬集中化相關規定。(修正規定第六點)

六、 因應系統防護需要，增列自管中心將日誌傳送管理層進行監控聯防規定。(修正規定第七點)

七、 依公文電子交換系統最新架構，新增交換層對所屬機關層辦理稽核作業規定。(修正規定第九點)

八、 為順遂管理層及交換層機關辦理中止機關(構)系統服務作業，增訂中止服務流程規定;因應管理實務需要，新增得中止機關(構)系統服務之違規情形及資通安全管理法主管機關通知發生重大危害資安事故之機關(構) 中止服務規定。(修正規定第十三點)

九、 配合第五點刪除天元模組使用管理及終端層機關連線異動申請表格式規定，刪除附錄一「公文 G2B2C 資訊服務中心連線異動申請表」、附錄二「天元模組遺失毀損報告單」、附錄三「天元模組緊急狀況處置報告單」;配合第九點增列交換層對所屬機關層辦理稽核作業需要，增列附錄二「公文電子交換系統(交換層對機關層)資訊安全稽核彙整表」; 配合第十三點增訂中止服務流程規定，增列附錄四「公文電子交換系統用戶中止服務流程」; 原附錄四及附錄五依序調整序號為附錄一及附錄三，並配合修正內容。

公文電子交換系統資訊安全管理規範
修正對照表

修正規定	現行規定	說明
一、為使公文電子交換系統（以下簡稱本系統）環境正常運作，確保本系統之機密性、完整性及安全性，特訂定本規範。	一、為使公文電子交換系統（以下簡稱本系統）環境正常運作，確保本系統之機密性、完整性及安全性，特訂定本規範。	本點未修正。
二、本規範主要依據如下： (一)公文程式條例。 (二)電子簽章法。 (三)資通安全管理法及相關子法。 (四)機關公文電子交換作業辦法。 (五)行政院及所屬各機關資訊安全管理要點。 (六)行政院及所屬各機關資訊安全管理規範。 (七)文書及檔案管理電腦化作業規範。	二、本規範主要依據如下： (一)公文程式條例。 (二)電子簽章法。 (三)機關公文電子交換作業辦法。 (四)行政院及所屬各機關資訊安全管理要點。 (五)行政院及所屬各機關資訊安全管理規範。 (六)文書及檔案管理電腦化作業規範。	第三款新增。規定資通安全管理法及相關子法為本規範之法令依據，以下各款款次順移。
三、本規範適用於依機關公文電子交換作業辦法進行文書傳遞交換作業之中央及地方各級機關(構)、公立學校、公營事業機構、行政法人、法人或非法人團體等(以下簡稱各機關(構))。	三、本規範適用於依機關公文電子交換作業辦法進行文書傳遞交換作業之政府機關（以下簡稱各機關），包括中央及地方各級機關(構)、公立學校、公營事業機構及行政法人等。	人民團體、商工企業及醫療院所等非政府機關用戶亦運用公文電子交換系統，與政府機關往來密切，考量國家整體資訊安全，爰將上開用戶納入本規範適用對象（檔案局一百零七年四月二十六日檔資字第一０七０００八一七六號函參照）。
四、本系統架構，區分為四個層級，定義如下： (一)管理層：指由國家發展委員會檔案管理局(以下簡稱檔案局)主管之公文G2B2C資訊服務中心。 (二)交換層：指由中央部會及直轄市政府、縣（市）政府等主管之公文統合交換中心(以下簡稱交換中心)	四、本系統架構，區分為三個層級，定義如下： (一)管理層：指由國家發展委員會檔案管理局(以下簡稱檔案局)主管之G2B2C公文交換中心。 (二)交換層：指由中央部會及直轄市政府、縣（市）政府等主管之公文統合交換中心。依開發維運型態，	一、依據公文電子交換系統最新架構，修正系統層級為四層級。 二、G2B2C公文交換中心名稱修正。 三、第三款新增。依據公文電子交換系統最新四層級架構，新增機關層定義。如某機關負責建置公文管理系統供所屬機關使用，該機關屬機關層機關。

。依開發維運型態，分為下列三種交換中心： 1. 共用中心：指由檔案局開發公文交換程式，並建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。 2. 自管中心：指使用檔案局開發之公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。 3. 自建中心：指自行或委外開發公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。 (三)機關層：指負責公文管理系統或其他應用系統且與交換層介接，以進行電子公文傳遞作業者。 (四)終端層：指由各機關(構)使用本系統進行公文電子交換收發文作業之終端用戶。	分為下列三種交換中心： 1. 共用中心：指由檔案局開發公文交換程式，並建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關進行公文電子交換者。 2. 自管中心：指使用檔案局開發之公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關進行公文電子交換者。 3. 自建中心：指自行或委外開發公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關進行公文電子交換者。 (三)終端層：指由各機關及單位使用本系統進行公文電子交換之終端用戶。	四、現行規定第三款款次順移。依據公文電子交換系統最新架構，酌修文字。
五、各機關(構)應依其於本系統架構之層級，辦理下列事項： (一)共通性安全事項： 1. 主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測	五、各機關(單位)應依其於本系統架構之層級，辦理下列事項：	一、第一款新增。規定各機關使用公文電子交換系統之共通管理事項如下： (一)主機防毒及漏洞修補作業。 (二)主機禁止安裝點對點(P2P)、即時通訊(IM)

有無感染電腦病毒。 2. 主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。 3. 當偵測到惡意程式等警訊時，應先行阻絕惡意程式，並暫停相關主機服務，避免惡意程式蔓延至其他交換層及機關層，並追查惡意程式來源，通知來源機關(構)儘速處理。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。 4. 應檢查主機安裝之伺服器應用軟體憑證及機關(構)使用之憑證IC卡效期，並於憑證效期過期前更新憑證，避免交換異常。 5. 應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。 6. 應使用並妥善保管管理層發交之密碼模組I辦理公文電子交換作業。 7. 本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。		、社交軟體或來源不明之網路應用程式，以及有關網路芳鄰使用規定。 (三)系統資安事件通報作業。 (四)憑證效期維護作業。 (五)系統校時作業。 (六)密碼模組導入使用。 (七)政府組態基準(GCB)導入作業。

(二)管理層機關：負責規劃、推動本系統發展與維護等安全管理事項，確保業務永續運作，包括： 1. 負責本系統程式之開發設計，納入密碼原則、資料有效性檢核及資料加密防護等安全性考量，並確保未被植入惡意程式。 2. 定期審視作業系統漏洞修補訊息，評估作業系統變更對本系統運作及安全產生之影響，並依據評估及測試結果，對本系統做必要調整，再進行作業系統變更，並對交換層發布作業系統更新通知。 3. 建立本系統程式版本控制及安全更版機制，更版之版本應以憑證簽章，確保更版過程未經竄改。 4. 對交換層及機關層主機之作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組態設定等作為系統安全維護設定之準則。 5. 本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，除非必要，應禁止與網際網路進行連線。 6. 配合各交換層主機IP	(一)管理層機關：負責規劃、推動本系統之電腦系統、網路、系統發展與維護、委外、憑證及教育訓練等安全管理事項，確保業務永續運作，包括： 1. 負責本系統程式之開發設計，納入密碼原則、資料有效性檢核及資料加密防護等安全性考量，並確保未被植入惡意程式。 2. 定期審視作業系統漏洞修補訊息，評估作業系統變更對本系統運作及安全產生之影響，並依據評估及測試結果，對本系統做必要調整，再進行作業系統變更，並對交換層發布作業系統更新通知。 3. 建立本系統程式版本控制及安全派送機制，派送之版本應以憑證簽章，確保派送過程未經竄改。 4. 對交換層及終端層主機之作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組態設定等作為系統安全維護設定之準則。 5. 本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，除非必要，應禁止與網際網路進行連線。 6. 配合各交換層主機IP位址之變動，更新交換	二、原第一款款次順移至第二款並簡化文字。各目修正說明如下： (一)配合公文電子交換系統機關層做法，酌修第三目相關文字。 (二)配合公文電子交換系統最新架構，原終端層介接公文電子交換系統作業改由機關層負責，爰修正第四目規定。 (三)原第八目移列為第一款共通性安全事項，爰刪除之。 (四)原第九目目次順移至第八目。 (五)原第十目目次順移至第九目，配合公文電子交換系統最新架構，調整相關文字。 (六)原第十一目目次順移至第十目，增加依原碼檢測及滲透測試結果進行必要修補作業之規定。 (七)原第十二目目次順移至第十一目。 (八)原第十三目目次順移至第十二目，考量公文電子交換系統管理維護教育訓練內容設計之彈性，爰刪除資訊安全(含個人資料保護)議題基本時數規定。 (九)第十三目新增，鑑於管理層為公文電子交換系統架構之重要功能，爰增列系統防護控制措施及委外規定。

位址之變動，更新交換主機IP位址清單，並據以修正防火牆白名單設定，同時通知各交換層機關。 7. 具有防範本系統主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。 8.訂定本系統安全傳輸協定，確保傳遞過程全程加密，並建立收發文確認機制，防止未經授權之資料存取及竄改。 9.定期進行本系統之網頁及主機弱點掃描並就掃描結果予以修補，且同時更新交換層及機關層相關程式。 10.定期辦理原碼檢測及滲透測試，或定期辦理資訊安全健檢，並進行必要之修補作業以預防或發現未知之威脅或攻擊。 11. 系統開發與維運工程師每年至少接受六小時安全程式撰寫技術及駭客攻擊手法攻防等資訊安全課程。 12. 每年辦理之本系統管理維護教育訓練應包含資訊安全(含個人資料保護)議題。 13. 至少應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理本系統維護作業，委	主機IP位址清單，並據以修正防火牆白名單設定，同時通知各交換層機關。 7. 具有防範本系統主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。 8. 安裝防毒軟體，並定期更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。 9.訂定本系統安全傳輸協定，確保傳遞過程全程加密，並建立收發文確認機制，防止未經授權之資料存取及竄改。 10. 定期辦理網頁及主機弱點掃描，並就掃描結果予以修補，且同時更新交換層及終端層相關程式。 11. 定期辦理原碼檢測及滲透測試，或定期辦理資訊安全健檢，以預防或發現未知之威脅或攻擊。 12. 系統開發與維運工程師每年至少接受六小時安全程式撰寫技術及駭客攻擊手法攻防等資訊安全課程。 13. 每年辦理之本系統管理維護教育訓練應有三分之一課程時數為資訊安全(含個人資料保護)議題。	

外作業應依資通安全管理法施行細則第四條規定辦理。 (三)交換層機關:負責交換層交換中心之運作與督導所屬機關層及終端層使用者交換作業等安全管理事項，包括： 1. 配合管理層發布之作業系統更新及漏洞修補通知，於一週內排定更新及修補時程，並儘速完成更新。 2. 應於接獲本系統更版通知後，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。 3. 本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，除非必要，應禁止與網際網路進行連線。 4. 依據管理層通知之交換主機IP位址清單進行防火牆白名單設定，並以一對一固定IP位址為原則，如有交換主機IP位址異動需求，應通知管理層辦理連線異動事宜。 5. 交換層機關應以防火牆白名單控管機關層及網頁版公文收發模組用戶連線作業，並以一對一固定IP位址為原則，如機關層及網頁版公文收發模組用戶有IP位址異動需	(二)交換層機關:負責交換層公文統合交換中心與督導所屬終端層使用者之電腦系統、網路、委外、憑證及教育訓練等安全管理事項，包括： 1. 配合管理層發布之作業系統更新通知，於一週內排定更新時程，並儘速完成更新。 2. 應於接獲本系統更版通知後，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。 3. 本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，除非必要，應禁止與網際網路進行連線。 4. 依據管理層通知之交換主機IP位址清單及所屬各終端層主機IP位址，進行防火牆白名單設定，並以一對一固定IP位址為原則；確有一對多或非固定IP位址之需求者，須向交換層機關申請核備，並應建立IP位址與機關名稱對照表，以供追蹤及查檢之用。 5. 具有防範公文電子交換主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。	三、原第二款款次順移至第三款，其修正說明如下： (一)簡化文字並增列機關層為交換層機關督導對象。 (二)第四目係規範交換層主機IP異動通報管理層作業，並新增交換主機IP位址異動應通知管理層辦理連線異動事宜，後段移列至第五目，爰刪除與該項作業無關之規定文字。 (三)新增第五目，增列交換層機關白名單控管機關層及網頁版公文收發模組用戶連線作業相關規定。 (四)原第五目目次順移至第六目。 (五)原第六目及第七目移列為第一款共通性安全事項，爰刪除。 (六)原第八目目次順移至第七目，酌修文字。 (七)依據公文電子交換系統架構，終端層多數安全管理事項向上集中至機關層，並考量機關(構)業務實際需求，公文電子交換系統資訊安全教育訓練作業改由各機關(構)依內部資訊安全規定辦理，故不再由本規範規定，爰刪除原第九目規定。 (八)第八目新增，增修交換層機關提供網頁

求，應通知交換層辦理連線異動事宜；確有一對多或非固定IP位址之需求者，應向交換層機關申請核准，並應建立IP位址與機關(構)名稱對照表，以供追蹤及查檢之用。 6. 具有防範公文電子交換主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。 7. 定期進行本系統之網頁及主機弱點掃描，並將掃描結果提供管理層研析。 8. 交換層機關提供網頁版公文收發模組介接使用本系統，應依本規範之要求辦理管理作業。 9. 至少應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理本系統維護作業，委外作業應依資通安全管理法施行細則第四條規定辦理。	6. 安裝防毒軟體，並定期更新病毒碼，對於收發公文及其附件進行掃描，偵測有無感染電腦病毒。 7. 當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並中止該公文之發送，避免惡意程式蔓延至其他交換層及終端層，並追查惡意程式來源，通知來源機關(單位)儘速處理惡意程式。如發生資安事件時，應儘速通知管理層，並採取必要之因應控管措施。 8. 定期進行網頁及主機弱點掃描，並將掃描結果提供管理層研析。 9. 每年應對所屬終端層機關(單位)收發人員辦理至少一小時之本系統資訊安全教育訓練課程。	版公文收發模組，其安全管理作業仍應依交換層及共通性安全規定事項辦理。 (九)第九目新增，鑑於交換層為公文電子交換系統架構之重要功能，爰增列系統防護控制措施及委外規定。
(四)機關層機關(構)：負責機關層公文交換相關軟硬體設施之安全管理，包括： 1. 於接獲本系統更版通知，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。 2. 機關層主機應專機專用並採用固定IP位址，因特殊理由未能遵		四、第四款新增，規定機關層機關安全管理事項。

行者，應採取必要之監管措施，並提報交換層機關備查。如有主機IP位址異動需求，亦應通知交換層機關以進行白名單之設定。 3. 定期進行本系統之網頁及主機弱點掃描，並將掃描結果提供管理層研析。 (五)終端層機關(構)：負責終端用戶本身之公文交換相關軟硬體設施之安全管理，包括： 1. 機關(構)如有資訊異動(例如機關(構)代碼、機關(構)名稱、電子憑證IC卡等)或機關(構)裁撤情形，應依管理層發布之程序辦理連線異動事宜。 2. 系統登錄註冊之電子憑證IC卡應專卡專用，並指定專人保管，未使用時應上鎖收存，以防止遺失。	(三)終端層機關(單位)：負責終端用戶公文交換主機電腦(含使用API介接交換系統之公文管理系統主機)、網路、委外及憑證等之安全管理，包括： 1. 作業系統應定期進行漏洞修補。 2. 安裝防毒軟體，並定期更新病毒碼，對於收發公文及其附件進行掃描，偵測有無感染電腦病毒。 3. 於接獲本系統更版通知後進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。 4. 終端層主機應專機專用並採用固定IP位址，因特殊理由未能遵行者，應採取必要的監管措施，並提報上級主管機關備查。 5. 機關(單位)如有資訊異動(例如IP位址、機關代碼、機關名稱、機關憑證、機關地址等)或機關裁撤情形，應填寫連線異動申請表(如附錄一)辦理連線異動事宜。 6. 終端層主機應禁止安	五、原第三款款次順移至第五款，其修正說明如下： (一)簡化文字，並依據公文電子交換系統最新架構，使用API介接公文電子交換系統作業非屬終端層權責，爰刪除相關文字。 (二)原第一目及第二目移列為第一款共通性安全事項，爰刪除。 (三)依據公文電子交換系統最新架構，終端層機關(構)非統一採用管理層開發之交換程式，爰刪除第三目規定。 (四)依據公文電子交換系統最新架構，原終端層介接公文電子交換系統作業改由機關層負責，爰刪除第四目規定。 (五)原第五目移列為第一目。鑑於機關層IP異動設定作業係依其所介接交換中心管理機關之規定程序辦理，且機關(構)地址非公文電子交換系統必要資訊及公

	裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。 7. 終端層使用機關(單位)每半年應至少執行備份或封存作業一次，以確保個人電腦系統安全。 8. 系統登錄註冊之電子憑證IC卡應專卡專用，並指定專人保管，未使用時應上鎖收存，以防止遺失。 9. 各機關負責公文收發之人員每年應接受至少一小時之公文電子交換系統資訊安全教育訓練課程。	文電子交換系統非僅支援機關憑證，刪除及修正相關規定內容。考量依管理實務，機關連線異動申請需依共用中心、自管中心及自建中心之實際運作模式而有不同申請程序及書表設計，故不再於本規範訂定統一格式，後續將由管理層依交換中心實際需要另行公布更新申請表格式，爰刪除附錄一。 (六)原第六目移列為第一款共通性安全事項，爰刪除。 (七)鑑於新系統架構下，終端層機關備份及封存作業對象非屬公文電子交換系統範圍，爰刪除第七目規定。 (八)原第八目目次調整至第二目。 (九)依據公文電子交換系統最新架構，終端層安全管理事項多數向上集中至機關層，並考量機關業務實際需求，公文電子交換系統資訊安全教育訓練作業改由各機關依內部資訊安全規定辦理，不再由本規範統一規定，爰刪除第九目規定。
(六)自建中心之機關具備管理層、交換層及機關層角色，應依本規範之要求，與本系統進行安全介接。	(四)自建中心之機關具備管理層及交換層角色，應依本規範之要求，與本系統進行安全介接。	六、原第四款款次順移，依據公文電子交換系統最新架構新增機關層角色，自建中心機關得依其實際情形適用機關層相

		關規定。
(七)機關層及終端層機關(構)使用共用中心或他機關自管、自建中心，其所隸之中央部會或直轄市政府、縣（市）政府對本規範要求事項應盡管理及督導之責。	(五)終端層機關使用共用中心或他機關自管中心，其所隸之中央部會或直轄市政府、縣（市）政府對本規範要求事項應盡管理及督導之責。	七、原第五款款次順移，依現行機關使用他機關交換中心現況，將交換層自建中心及機關層機關納入適用對象。
	(六)機關應使用檔案局發交之密碼模組I(採軟體式加解密元件) 或天元模組(採硬體式加解密元件)辦理公文電子交換作業。使用天元模組之機關應遵守下列管理規定: 1.模組使用： 本模組僅限政府機關公文電子交換系統使用。 2.模組存管： (1) 領用模組應完備交接程序，詳實登載帳籍，並每季清點模組料帳是否相符。 (2) 應指定專人保管，落實職務代理及業務交接規定；未使用時應上鎖收存，以防遺失。 (3) 如有帳籍異動、新申請使用或繳回模組等需求，應通報檔案局辦理。 3.模組維保： (1) 模組遇故障、異常或鎖卡導致無法正常運作時，應先向檔案局反映並尋求支援協	八、鑑於新公文電子交換系統不再使用天元模組，統一採用密碼模組I，並於共通性安全事項另訂密碼模組I使用規定，爰刪除原第六款規定，並刪除附錄二及附錄三。

	助，如仍無法處理，應與國家安全局(以下簡稱國安局)客服中心聯繫，嚴禁私自或委外拆解及維修。 (2) 備用模組之啟用應先通報檔案局同意。 (3) 為確保模組正常運作，國安局得視模組妥善情況，赴使用單位實施現地維保檢測，使用單位應配合國安局人員進行相關維保作業。 4.模組緊急狀況處置： (1) 發生模組遺失或毀損情事時，應查明遺毀原因，並於三日內填具「天元模組遺失毀損報告單」(如附錄二) 送檔案局轉密碼作業督導機關行政院(外交國防法務處)憑辦。除屬不可抗力之原因外，使用者應善盡保管之責，若發生遺失或惡意毀損情事，應追究其責任並辦理賠償，賠償金額依財物單價乘以剩餘使用時間與財物耐用年數比率計算。賠償程序由國安局另定之。 (2) 機關遇不可抗力	

	之因素(如颱風、火災、水災、恐怖攻擊等)致無法保存模組於機關內時，得指派專人攜離模組或逕將模組毀壞，並應於三日內填具「天元模組緊急狀況處置報告單」(如附錄三)送檔案局轉密碼作業督導機關行政院(外交國防法務處)通報國安局。 5.其他注意事項： (1) 本模組使用USB介面與電腦連結使用，使用人員應依循單位資訊安全政策，申請資訊媒體及USB周邊設備開放相關事宜。 (2) 本模組僅提供資料加密保護，未具其他資安防護功能。	
六、本系統各層級機關(構)，基於組織改造及政府資訊資源向上集中原則，應落實所轄範圍自主管理。	六、本系統各層級機關，基於組織改造及政府資訊資源向上集中原則，應落實所轄範圍自主管理，管理層及交換層應逐步朝虛擬集中化發展建立最適經濟規模之公文電子交換架構。	鑑於最新公文電子交換系統架構已達虛擬集中化之最適經濟規模，爰刪除相關規定。
七、為確保機關(構)對外公務連繫順暢安全無慮，各機關(構)應將本系統納入機關(構)內部或參採所屬上級機關(構)	七、為確保機關對外公務連繫順暢安全無慮，各機關應將本系統納入機關內部或參採所屬上級機關之資訊安全管	一、增列主機及應用系統日誌(log)監控為資安監控中心防護範圍。 二、新增第二項，增列自管中心將日誌傳送管理層

之資訊安全管理系統(ISMS)管理；管理層及交換層機關應將本系統納入ISMS第三方認證範圍與資安監控中心(SOC)監控防護範圍，防護標的應包含主機及應用系統日誌(log)監控。 自管中心應將日誌傳送管理層，以強化聯防機制，如自管中心為實體隔離環境，則應依管理層提供之監控規則進行布署設定。	理系統(ISMS)管理；管理層及交換層機關應將本系統納入ISMS第三方認證範圍與資安監控中心(SOC)監控防護範圍。	進行監控聯防規定。
八、管理層及交換層機關應將本系統納入年度資安稽核計畫，並依附錄一「公文電子交換系統資訊安全自評表」辦理自評，對於不符合事項應即時改善，並附佐證說明。	八、管理層及交換層機關應將本系統納入年度資安稽核計畫，並依附錄四「公文電子交換系統資訊安全自評表」辦理自評，對於不符合事項應即時改善，並附佐證說明。	修正附錄四並變更其序號為附錄一。
九、交換層機關經評估資訊安全風險程度，得採全面性或抽查方式對所屬機關層及終端層機關(構)進行定期稽核，對於不符合事項應要求即時改善及追蹤改善情形；並於每年十一月三十日前彙整對所屬機關(構)之稽核結果(如附錄二及三)，併同本機關交換層自評表送交管理層機關。對嚴重不符事項或特殊資訊安全事件，應不定期進行專案稽核作業。	九、交換層機關經評估資訊安全風險程度，得採全面性或抽查方式對所屬終端層機關(單位)進行定期稽核，對於不符合事項應要求即時改善及追蹤改善情形；並於每年十一月底前彙整對所屬機關(單位)之稽核結果(如附錄五)，併同本機關交換層自評表送交管理層機關。對嚴重不符事項或特殊資訊安全事件，應不定期進行專案稽核作業。	增列機關層機關為交換層機關稽核對象。另新增附錄二及修正附錄五改列為附錄三。
十、管理層機關得召集學者專家成立公文電子交換資訊安全稽核小組，對交換層機關進行定期稽核或專案稽核作	十、管理層機關得召集學者專家成立公文電子交換資訊安全稽核小組，對交換層機關進行定期稽核或專案稽核作	本點未修正。

業，以確保公文電子交換網路環境之資訊安全。	業，以確保公文電子交換網路環境之資訊安全。	
十一、各機關(構)應依自評及稽核結果，對執行本系統資訊安全工作績優或缺失人員，予以適當獎懲。管理層及交換層機關得對執行本系統資訊安全工作績優或缺失之機關(構)人員(含所屬機關(構))，予以適當之獎懲建議。	十一、各機關應依自評及稽核結果，對執行本系統資訊安全工作績優或缺失人員，予以適當獎懲。管理層及交換層機關得對執行本系統資訊安全工作績優或缺失之機關人員(含所屬機關)，予以適當之獎懲建議。	配合第三點修正規定，酌修文字。
十二、各機關(構)應依本規範相關規定，納入系統委外契約履約之事項，並定明相關法律責任。委外人員如有違反者，各機關(構)應確實依契約約定辦理。	十二、各機關應依本規範相關規定，納入系統委外契約履約之事項，並定明相關法律責任。委外人員如有違反者，機關應確實依契約約定辦理。	配合第三點修正規定，酌修文字。
十三、管理層及交換層機關因資訊安全需求，請使用機關(構)配合調查或辦理事項，各使用機關(構)應於期限內完成。 各機關(構)如有發生下列情形之一者，其所屬之交換層機關或管理層機關得依附錄四「公文電子交換系統用戶中止服務流程」中止對該機關(構)之系統服務： (一)發生資通安全事件通報及應變辦法所列第三級至第四級資通安全事件。 (二)電子憑證IC卡遺失或未使用加解密模組。 (三)機關(構)未將本系統	十三、管理層及交換層機關因資訊安全需求，請使用機關配合調查或辦理事項，各使用機關應於期限內完成。 機關如有發生下列情形之一者，其所屬之交換層機關或管理層機關得中止對該機關之系統服務： (一)發生國家資通安全通報應變作業綱要所列第三級至第四級資安事件。 (二)電子憑證IC卡效期過期或遺失或軟/硬體加解密模組或設備遺失。 (三)機關未將本系統納入機關內部或參採所隸	一、文字酌修，另為順遂機關辦理中止機關系統服務作業，增訂中止服務流程規定，新增附錄四。 二、鑑於資通安全管理法施行，行政院業依該法第十四條規定訂頒資通安全事件通報及應變辦法以資機關辦理資通安全事件通報及應變作業遵循，並以一百零八年三月五日院臺護字第一〇八〇一六六九六〇號函公告停止適用「國家資通安全通報應變作業綱要」，爰修正第一款引用規定。 三、配合第五點第六款規定刪除，酌修第二款相關文字。 四、參採檔案局訂定之「公

納入機關內部或參採所隸上級機關(構)之資訊安全管理系統(ISMS)管理。 (四)交換層機關未將本系統納入ISMS第三方認證範圍與資安監控中心(SOC)監控範圍防護。 (五)未依規定辦理本系統資訊安全自評或未對所屬終端層機關(構)進行定期稽核。 (六)拒絕接受管理層或交換層機關稽核或拒絕依稽核結果限期改善。 (七)發送廣告性質電子公文經交換層機關警告後仍未改善。 (八)利用本系統散播電腦病毒。 (九)蓄意破壞、干擾或妨礙其他用戶之交換系統，或對交換層主機持續進行阻斷性攻擊。 (十)發送侵害他人智慧財產權之電子公文或附件檔。 (十一)未即時改善不符合事項且無正當理由者。 (十二)其他未依本規範規定執行工作權責且情節重大。 交換系統用戶機關(構)之公文相關系統發生資安事件，經資通安全管理法主管機關依資通安全事件通報及應變辦法規定程序認定有重大危害之虞者，得通知管理層及交	上級機關之資訊安全管理系統(ISMS)管理。 (四)交換層機關未將本系統納入ISMS第三方認證範圍與資安監控中心(SOC)監控範圍防護。 (五)未依規定辦理公文電子交換系統資訊安全自評或未對所屬終端層機關(單位)進行定期稽核。 (六)拒絕接受管理層或交換層機關稽核或拒絕依稽核結果限期改善。 (七)發送廣告性質電子公文經交換層機關警告後仍未改善。 (八)未即時改善不符合事項且無正當理由者。 (九)其他未依本規範規定執行工作權責且情節重大。	文電子交換系統用戶中止服務作業指引」，新增本項第八至十款得中止系統服務之情形。 五、原第八款、第九款款次順移至第十一款、第十二款。 六、鑑於機關(構)資安事故如屬經資通安全管理法主管機關依資通安全事件通報及應變辦法第十七條規定程序認定具有重大危害者，應有更為及時之中止服務作業方式，以防止損害迅速擴散，爰增列第三項規定。

換層機關中止該用戶系統服務；資安事件處理完竣，經資通安全管理法主管機關確認及通知後，始得復原系統服務。		
十四、本規範未訂定事項，依資通安全管理法、行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範等相關規定辦理。	十四、本規範未訂定事項，依行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範等相關規定辦理。	新增資通安全管理法為本規範之補充規定。

公文電子交換系統資訊安全管理規範

中華民國 103 年 2 月 5 日行政院院授發檔(資)字第 1030008043 號函頒布
中華民國 105 年 4 月 29 日行政院院授發檔(資)字第 1050008272 號函頒修正
中華民國 108 年 11 月 15 日行政院院授發檔(資)字第 1080008553 號函修正

壹、總則

一、為使公文電子交換系統（以下簡稱本系統）環境正常運作，確保本系統之機密性、完整性及安全性，特訂定本規範。

二、本規範主要依據如下：

(一)公文程式條例。

(二)電子簽章法。

(三)資通安全管理法及相關子法。

(四)機關公文電子交換作業辦法。

(五)行政院及所屬各機關資訊安全管理要點。

(六)行政院及所屬各機關資訊安全管理規範。

(七)文書及檔案管理電腦化作業規範。

三、本規範適用於依機關公文電子交換作業辦法進行文書傳遞交換作業之中央及地方各級機關(構)、公立學校、公營事業機構、行政法人、法人或非法人團體等(以下簡稱各機關(構))。

四、本系統架構，區分為四個層級，定義如下：

(一) 管理層：指由國家發展委員會檔案管理局(以下簡稱檔案局)主管之公文 G2B2C 資訊服務中心。

(二) 交換層：指由中央部會及直轄市政府、縣（市）政府等主管

之公文統合交換中心(以下簡稱交換中心)。依開發維運型態，分為下列三種交換中心：

1. 共用中心：指由檔案局開發公文交換程式，並建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。
2. 自管中心：指使用檔案局開發之公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。
3. 自建中心：指自行或委外開發公文交換程式，自行建置硬體設備環境、負責設備維運及軟體使用管理，提供使用機關(構)進行公文電子交換者。

(三) 機關層：指負責公文管理系統或其他應用系統且與交換層介接，以進行電子公文傳遞作業者。

(四) 終端層：指由各機關(構)使用本系統進行公文電子交換收發文作業之終端用戶。

貳、機關權責

五、各機關(構)應依其於本系統架構之層級，辦理下列事項：

(一) 共通性安全事項：

1. 主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。
2. 主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。
3. 當偵測到惡意程式等警訊時，應先行阻絕惡意程式，並暫停

相關主機服務，避免惡意程式蔓延至其他交換層及機關層，並追查惡意程式來源，通知來源機關(構)儘速處理。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。

4. 應檢查主機安裝之伺服器應用軟體憑證及機關(構)使用之憑證 IC 卡效期，並於憑證效期過期前更新憑證，避免交換異常。
5. 應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。
6. 應使用並妥善保管管理層發交之密碼模組 I 辦理公文電子交換作業。
7. 本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。

(二) 管理層機關：負責規劃、推動本系統發展與維護等安全管理事項，確保業務永續運作，包括：

1. 負責本系統程式之開發設計，納入密碼原則、資料有效性檢核及資料加密防護等安全性考量，並確保未被植入惡意程式。
2. 定期審視作業系統漏洞修補訊息，評估作業系統變更對本系統運作及安全產生之影響，並依據評估及測試結果，對本系統做必要調整，再進行作業系統變更，並對交換層發布作業系統更新通知。
3. 建立本系統程式版本控制及安全更版機制，更版之版本應以憑證簽章，確保更版過程未經竄改。

4. 對交換層及機關層主機之作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組態設定等作為系統安全維護設定之準則。
5. 本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，除非必要，應禁止與網際網路進行連線。
6. 配合各交換層主機 IP 位址之變動，更新交換主機 IP 位址清單，並據以修正防火牆白名單設定，同時通知各交換層機關。
7. 具有防範本系統主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。
8. 訂定本系統安全傳輸協定，確保傳遞過程全程加密，並建立收發文確認機制，防止未經授權之資料存取及竄改。
9. 定期進行本系統之網頁及主機弱點掃描並就掃描結果予以修補，且同時更新交換層及機關層相關程式。
10. 定期辦理原碼檢測及滲透測試，或定期辦理資訊安全健檢，並進行必要之修補作業，以預防或發現未知之威脅或攻擊。
11. 系統開發與維運工程師每年至少接受六小時安全程式撰寫技術及駭客攻擊手法攻防等資訊安全課程。
12. 每年辦理之本系統管理維護教育訓練應包含資訊安全(含個人資料保護)議題。
13. 至少應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理本系統維護作業，委外作業應依資通安全管理法施行細則第四條規定辦理。

(三) 交換層機關: 負責交換層交換中心之運作與督導所屬機關層及終端層使用者交換作業等安全管理事項，包括：

1. 配合管理層發布之作業系統更新及漏洞修補通知，於一週內排定更新及修補時程，並儘速完成更新。
2. 應於接獲本系統更版通知後，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。
3. 本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，除非必要，應禁止與網際網路進行連線。
4. 依據管理層通知之交換主機 IP 位址清單進行防火牆白名單設定，並以一對一固定 IP 位址為原則，如有交換主機 IP 位址異動需求，應通知管理層辦理連線異動事宜。
5. 交換層機關應以防火牆白名單控管機關層及網頁版公文收發模組用戶連線作業，並以一對一固定 IP 位址為原則，如機關層及網頁版公文收發模組用戶有 IP 位址異動需求，應通知交換層辦理連線異動事宜；確有一對多或非固定 IP 位址之需求者，應向交換層機關申請核准，並應建立 IP 位址與機關(構)名稱對照表，以供追蹤及查檢之用。
6. 具有防範公文電子交換主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。
7. 定期進行本系統之網頁及主機弱點掃描，並將掃描結果提供管理層研析。
8. 交換層機關提供網頁版公文收發模組介接使用本系統，應依本規範之要求辦理管理作業。

9. 至少應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理本系統維護作業，委外作業應依資通安全管理法施行細則第四條規定辦理。

(四) 機關層機關(構)：負責機關層公文交換相關軟硬體設施之安全管理，包括：

1. 於接獲本系統更版通知，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。
2. 機關層主機應專機專用並採用固定 IP 位址，因特殊理由未能遵行者,應採取必要之監管措施,並提報交換層機關備查。如有主機 IP 位址異動需求，亦應通知交換層機關以進行白名單之設定。
3. 定期進行本系統之網頁及主機弱點掃描，並將掃描結果提供管理層研析。

(五) 終端層機關(構)：負責終端用戶本身之公文交換相關軟硬體設施之安全管理，包括：

1. 機關(構)如有資訊異動(例如機關(構)代碼、機關(構)名稱、電子憑證 IC 卡等)或機關(構)裁撤情形,應依管理層發布之程序辦理連線異動事宜。
2. 系統登錄註冊之電子憑證 IC 卡應專卡專用,並指定專人保管，未使用時應上鎖收存，以防止遺失。

(六) 自建中心之機關具備管理層、交換層及機關層角色，應依本規範之要求，與本系統進行安全介接。

(七) 機關層及終端層機關(構)使用共用中心或他機關自管、自建中心，其所隸之中央部會或直轄市政府、縣（市）政府對本

規範要求事項應盡管理及督導之責。

六、本系統各層級機關(構)，基於組織改造及政府資訊資源向上集中原則，應落實所轄範圍自主管理。

七、為確保機關(構)對外公務連繫順暢安全無慮，各機關(構)應將本系統納入機關(構)內部或參採所屬上級機關(構)之資訊安全管理系統(ISMS)管理；管理層及交換層機關應將本系統納入 ISMS 第三方認證範圍與資安監控中心(SOC)監控防護範圍，防護標的應包含主機及應用系統日誌(log)監控。

自管中心應將日誌傳送管理層，以強化聯防機制，如自管中心為實體隔離環境，則應依管理層提供之監控規則進行布署設定。

參、自評及稽核

八、管理層及交換層機關應將本系統納入年度資安稽核計畫，並依附錄一「公文電子交換系統資訊安全自評表」辦理自評，對於不符合事項應即時改善，並附佐證說明。

九、交換層機關經評估資訊安全風險程度，得採全面性或抽查方式對所屬機關層及終端層機關(構)進行定期稽核，對於不符合事項應要求即時改善及追蹤改善情形；並於每年十一月三十日前彙整對所屬機關(構)之稽核結果(如附錄二及三)，併同本機關交換層自評表送交管理層機關。對嚴重不符事項或特殊資訊安全事件，應不定期進行專案稽核作業。

十、管理層機關得召集學者專家成立公文電子交換資訊安全稽核小組，對交換層機關進行定期稽核或專案稽核作業，以確保公文

電子交換網路環境之資訊安全。

肆、獎懲措施

十一、各機關(構)應依自評及稽核結果，對執行本系統資訊安全工作績優或缺失人員，予以適當獎懲。管理層及交換層機關得對執行本系統資訊安全工作績優或缺失之機關(構)人員(含所屬機關(構))，予以適當之獎懲建議。

十二、各機關(構)應依本規範相關規定，納入系統委外契約履約之事項，並定明相關法律責任。委外人員如有違反者，各機關(構)應確實依契約約定辦理。

伍、附則

十三、管理層及交換層機關因資訊安全需求，請使用機關(構)配合調查或辦理事項，各使用機關(構)應於期限內完成。

各機關(構)如有發生下列情形之一者，其所屬之交換層機關或管理層機關得依附錄四「公文電子交換系統用戶中止服務流程」中止對該機關(構)之系統服務：

(一) 發生資通安全事件通報及應變辦法所列第三級至第四級資通安全事件。

(二) 電子憑證 IC 卡遺失或未使用加解密模組。

(三) 機關(構)未將本系統納入機關內部或參採所隸上級機關(構)之資訊安全管理系統(ISMS)管理。

(四) 交換層機關未將本系統納入 ISMS 第三方認證範圍與資安監控中心(SOC)監控範圍防護。

(五) 未依規定辦理本系統資訊安全自評或未對所屬機關層及終端層機關(構)進行定期稽核。

(六) 拒絕接受管理層或交換層機關稽核或拒絕依稽核結果限期改善。

(七) 發送廣告性質電子公文經交換層機關警告後仍未改善。

(八) 利用本系統散播電腦病毒。

(九) 蓄意破壞、干擾或妨礙其他用戶之交換系統，或對交換層主機持續進行阻斷性攻擊。

(十) 發送侵害他人智慧財產權之電子公文或附件檔。

(十一)未即時改善不符合事項且無正當理由者。

(十二)其他未依本規範規定執行工作權責且情節重大。

交換系統用戶機關(構)之公文相關系統發生資安事件，經資通安全管理法主管機關依資通安全事件通報及應變辦法規定程序認定有重大危害之虞者，得通知管理層及交換層機關中止該用戶系統服務；資安事件處理完竣，經資通安全管理法主管機關確認及通知後，始得復原系統服務。

十四、本規範未訂定事項，依資通安全管理法、行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範等相關規定辦理。

附錄一　公文電子交換系統資訊安全自評表

編號	檢核項目		自評結果	相關佐證說明
1	管[1]	程式之開發設計應納入密碼原則、資料有效性檢核及資料加密防護等安全性考量，並確保未被植入惡意程式。	□符合 □部分符合 □不符合 □不適用	
2	管	定期審視作業系統漏洞修補訊息，評估作業系統變更對本系統運作及安全產生之影響，並依據評估及測試結果，對本系統做必要調整，再進行作業系統變更，並對交換層發布作業系統更新通知。	□符合 □部分符合 □不符合 □不適用	
	交	配合管理層發布之作業系統更新及漏洞修補通知，於一週內排定更新時程並儘速完成更新。		
3	管	建立本系統程式版本控制及安全更版機制，更版之版本應以憑證簽章，確保更版過程未經竄改。	□符合 □部分符合 □不符合 □不適用	
	交	於接獲本系統更版通知後，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。		
4	管	針對交換層及機關層主機作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組態設定等作為系統安全維護設定之準則。	□符合 □部分符合 □不符合 □不適用	
	交	依循作業環境標準組態列表進行設定。		
5	管	本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，非必要應禁止與網際網路進行連線。	□符合 □部分符合 □不符合 □不適用	
	交			
6	管	配合各交換層主機 IP 位址之變動，更新交換主機 IP 位址清單，並據以修正防火牆白名單設定，同時通知各交換層機關。	□符合 □部分符合 □不符合 □不適用	
	交	依據管理層通知之交換主機 IP 位址清單進行防火牆白名單設定，如有交換主機 IP 位址異動需求，應通知管理層辦理連線異動事宜。		
7	交	交換層機關應以防火牆白名單控管機關層及網頁版公文收發模組用戶連線作業，並以一對一固定 IP 位址為原則，如機關層及網頁版公文收發模組用戶有 IP 位址異動需求，應通知交換層辦理連線異動事宜；確有一對多或非固定 IP 位址之需求者，應向交換層機關申請核准，並應建立 IP 位址與機關(構)名稱對照表，以供追蹤及查檢之用。	□符合 □部分符合 □不符合 □不適用	
8	管	具有防範公文電子交換主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。	□符合 □部分符合 □不符合 □不適用	
	交			
9	管	主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。	□符合 □部分符合 □不符合 □不適用	
	交			

[1]以「管」、「交」分別標記為管理層及交換層之檢核項目

編號	檢核項目		自評結果	相關佐證說明
10	管	當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並暫停相關主機服務，避免惡意程式蔓延，並追查惡意程式來源，通知來源機關(構)儘速處理惡意程式。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。	□符合 □部分符合 □不符合 □不適用	
	交			
11	管	訂定本系統安全傳輸協定，確保傳遞過程全程加密，並建立收發文確認機制，防止未經授權之資料存取及竄改。	□符合 □部分符合 □不符合 □不適用	
12	管	定期進行本系統網頁及主機弱點掃描，並就掃描結果予以修補，且同時更新交換層及機關層相關程式。	□符合 □部分符合 □不符合 □不適用	
	交	定期進行本系統之網頁及主機弱點掃描，並將掃描結果提供管理層研析。		
13	管	定期辦理原碼檢測及滲透測試，或定期辦理資訊安全健檢，並進行必要之修補作業，以預防或發現未知之威脅或攻擊。	□符合 □部分符合 □不符合 □不適用	
14	管	系統開發與維運工程師每年至少接受六小時安全程式撰寫技術及駭客攻擊手法攻防等資訊安全課程。	□符合 □部分符合 □不符合 □不適用	
15	管	應檢查主機安裝之伺服器應用軟體憑證效期，並於憑證效期過期前更新憑證，避免交換異常。	□符合 □部分符合 □不符合 □不適用	
	交			
16	管	每年辦理之公文電子交換系統管理維護教育訓練應包含資訊安全(含個人資料保護)議題。	□符合 □部分符合 □不符合 □不適用	
17	管	應將公文電子交換系統納入 ISMS 第三方認證範圍與資安監控中心(SOC)監控範圍防護，SOC 監控範圍須包含主機及應用系統日誌（log）監控。 自管中心須將日誌傳送至管理層進行監控聯防，如自管中心為實體隔離環境，則須依管理層提供之監控規則進行布署設定。	□符合 □部分符合 □不符合 □不適用	
	交			
18	管	應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。	□符合 □部分符合 □不符合 □不適用	
	交			
19	管	主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。	□符合 □部分符合 □不符合 □不適用	
	交			
20	管	應使用並妥善保管管理層發交之密碼模組 I 辦理公文電子交換作業。	□符合 □部分符合 □不符合 □不適用	
	交			

編號	檢核項目		自評結果	相關佐證說明
21	管	本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。	□符合 □部分符合 □不符合 □不適用	
	交			
22	管	至少應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理本系統維護作業，委外作業應依資通安全管理法施行細則第四條規定辦理。	□符合 □部分符合 □不符合 □不適用	
	交			
23	交	交換層機關提供網頁版公文收發模組介接使用本系統，應依本規範之要求辦理管理作業。	□符合 □部分符合 □不符合 □不適用	
		總結：		

自評機關：

承辦人：　　聯絡電話：　　email:

單位主管：　　聯絡電話：　　email:

填表日期：

附錄二　公文電子交換系統(交換層對機關層)資訊安全稽核彙整表

□定期稽核：稽核日期：　　稽核機關(構)數：

稽核比例：□全面性 □抽檢　　%

□專案稽核：稽核日期：　　稽核機關(構)數：

稽核比例：□全面性 □抽檢　　%

專案稽核原因：

編號	檢核項目	符合數目	部分符合數目	不符合數目	不適用數目	相關佐證說明
1	主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。					
2	定期進行本系統之網頁及主機弱點掃描，並將掃描結果提供管理層研析。					
3	當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並暫停相關主機服務，避免惡意程式蔓延至其他交換層及機關層，並追查惡意程式來源，通知來源機關(構)儘速處理惡意程式。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。					
4	應檢查主機安裝之伺服器應用軟體憑證效期，並於憑證效期過期前更新憑證，避免交換異常。					
5	應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。					
6	於接獲本系統更版通知，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。					
7	機關層主機應專機專用並採用固定 IP 位址，因特殊理由未能遵行者，應採取必要之監管措施，並提報交換層機關核准。如有主機 IP 位址異動需求，亦應通知交換層機關以進行白名單之設定。					
8	主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。					

編號	檢核項目	符合數目	部分符合數目	不符合數目	不適用數目	相關佐證說明
9	應使用並妥善保管管理層發交之密碼模組Ⅰ辦理公文電子交換作業。					
10	本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。					
11	依循作業環境標準組態列表進行設定。					
總結：						

稽核機關：

承辦人：　　聯絡電話：　　email:

單位主管：　　聯絡電話：　　email:

填表日期：

備註：必要時得檢附個別機關之稽核結果。

附錄三　公文電子交換系統(交換層對終端層)資訊安全稽核彙整表

□定期稽核：稽核日期：　　稽核機關(構)數：

稽核比例：□全面性 □抽檢　%

□專案稽核：稽核日期：　　稽核機關(構)數：

稽核比例：□全面性 □抽檢　%

專案稽核原因：

編號	檢核項目	符合數目	部分符合數目	不符合數目	不適用數目	相關佐證說明
1	主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。					
2	機關(構)如有資訊異動(例如機關代碼、機關名稱、電子憑證 IC 卡等)或機關裁撤情形，應依管理層發布之程序辦理連線異動事宜。					
3	應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。					
4	系統登錄註冊之電子憑證 IC 卡應專卡專用，並指定專人保管，未使用時應上鎖收存以防止遺失，並於憑證效期過期前更新憑證 IC 卡，避免交換異常。					
5	主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。					
6	當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並暫停相關主機服務，避免惡意程式蔓延，並追查惡意程式來源，通知來源機關(構)儘速處理惡意程式。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。					
7	應使用並妥善保管管理層發交之密碼模組 I 辦理公文電子交換作業。					
8	本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。					
總結：						

稽核機關：

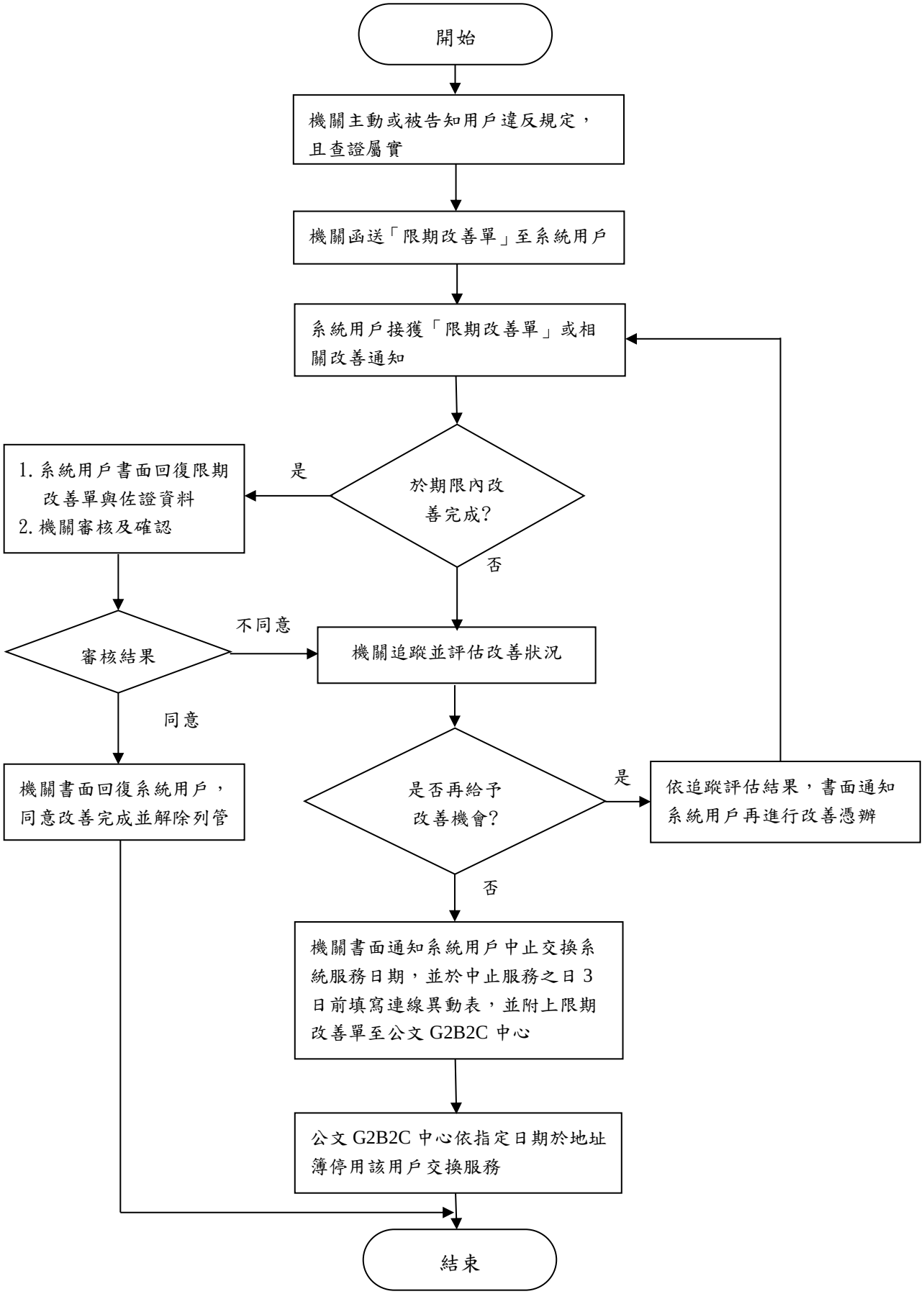
承辦人：　　聯絡電話：　　email:

單位主管：　　聯絡電話：　　email:

填表日期：

備註：必要時得檢附個別機關之稽核結果。

附錄四　公文電子交換系統用戶中止服務流程



※本流程之書面回復，得以正式公函、傳真或電子郵件方式為之。

附錄修正對照表

修 正 規 定	現 行 規 定	說明
	附錄一　公文G2B2C資訊服務中心連線異動申請表 **申請日期：　年　月　日** 機關代碼：　　U 機關全銜： 地址： 聯絡人：　　聯絡電話：	一、附錄一刪除。 二、配合第五點修正規定。

傳真電話		E-mail		
申請項目（請勾選左側項目並詳填右側相關資料）				
□機關聯絡資料異動	地　　址			
	聯 絡 人		聯絡電話	
	傳真電話		E-mail	
□取消交換	自年月日起永久取消電子交換			
□異動連線 IP	□統合交換中心	□eManager□eHub□eOldGW		

			舊 IP：　．　．　．　自年月日起更改 IP 為：　．　．　．	
	□機關改制			
	新機關代碼		U	
	新機關名稱			
	□更	憑證卡類別	□GCA　□XCA　□MOEACA	

	換機關憑證	卡憑證號		用戶啟用日期	年月日	
		卡憑證用途	□收發合一	□發文憑證 □收文憑證		

	申請機關章	備註	
	以下部分請勿填寫，由客服人員填寫		

<table>
<tr>
<td></td>
<td>
<table>
<tr><td colspan="4">客服處理情形說明</td></tr>
<tr><td>國家發展委員會檔案管理局審核</td><td></td><td>審核日期</td><td></td></tr>
<tr><td>公文中心審核</td><td></td><td>中心處理人員</td><td></td></tr>
</table>
※填寫完成後請傳真公文G2B2C資訊服務中心：(02)2513-6075客服專線：(02)2503-0030
</td>
<td></td>
</tr>
<tr>
<td>附錄一　公文電子交換系統資訊安全自評表</td>
<td>附錄四 公文電子交換系統資訊安全自評表</td>
<td>一、附錄序號變更。
二、配合第八點修正，附錄四變更其序號為附錄一。
三、配合修正規定第五點第三</td>
</tr>
</table>

編號	檢核項目		自評結果	相關佐證說明
1	管[1]	程式之開發設計應納入密碼原則、資料有效性檢核及資料加密防護等安全性考量，並確保未被植入惡意程式。	□符合 □部分符合 □不符合 □不適用	
2	管	定期審視作業系統漏洞修補訊息，評估作業系統變更對本系統運作及安全產生之影響，並依據評估及測試結果，對本系統做必要調整，再進行作業系統變更，並對交換層發布作業系統更新通知。	□符合 □部分符合 □不符合 □不適用	
	交	配合管理層發布之作業系統更新及漏洞修補通知，於一週內排定更新時程並儘速完成更新。		
3	管	建立本系統程式版本控制	□符合	

編號	檢核項目		自評結果	相關佐證說明
1	管[1]	程式之開發設計應納入密碼原則、資料有效性檢核及資料加密防護等安全性考量，並確保未被植入惡意程式。	□符合 □部分符合 □不符合 □不適用	
2	管	定期審視作業系統漏洞修補訊息，評估作業系統變更對本系統運作及安全產生之影響，並依據評估及測試結果，對本系統做必要調整，再進行作業系統變更，並對交換層發布作業系統更新通知。	□符合 □部分符合 □不符合 □不適用	
	交	配合管理層發布之作業系統更新通知，於一週內排定更新時程並儘速完成更新。		
3	管	建立本系統程式版本控制及安全派送機制，派送之版	□符合 □部分符	

款第一目規定，修正檢核項目二文字。

四、配合修正規定第五點第二款第三目規定，修正檢核項目三文字。

五、配合修正規定第五點第二款第四目規定，修正檢核項目四文字。

六、配合修正規定第五點第二款第六目及第三款第四目規定，修正檢核項目六文字。

七、配合修正規定第五點第三款第五目規定新增檢核項目七。

八、原檢核項目七、八項次順移至項目八、項目九。

九、原檢核項目九項次順移至項目十；配合修正規定第五點第一款第三目規定修正文字。

十、原檢核項目十項次順移至

		及安全更版機制，更版之版本應以憑證簽章，確保更版過程未經竄改。	□部分符合 □不符合 □不適用	
	交	於接獲本系統更版通知後，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。		
4	管	針對交換層及機關層主機作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組態設定等作為系統安全維護設定之準則。	□符合 □部分符合 □不符合 □不適用	
	交	依循作業環境標準組態列表進行設定。		
5	管	本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，非必要應禁止與網際網路進行連線。	□符合 □部分符合 □不符合 □不適用	
	交			
		本並應以憑證簽章，確保派送過程未經竄改。	□符合 □部分符合 □不符合 □不適用	
	交	於接獲本系統更版通知後，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。		
4	管	針對交換層及終端層主機作業環境建立標準組態列表，包括作業系統版本、套件版本及相關組態設定等作為系統安全維護設定之準則。	□符合 □部分符合 □不符合 □不適用	
	交	依循作業環境標準組態列表進行設定。		
5	管	本系統各項主機應專機專用，不得安裝非必要軟體，並以防火牆及其他必要安全設施，管控與其他主機間之資料傳輸及資源存取，非必要應禁止與網際網路進行連線。	□符合 □部分符合 □不符合 □不適用	
	交			
6	管	建立及維護交換主機 IP 位	□符合	

項目十一。

十一、原檢核項目十一項次順移至項目十二；配合修正規定第五點第二款第九目及同點第三款第七目規定修正文字。

十二、原檢核項目十二、十三項次順移至項目十三、項目十四。

十四、配合修正規定第五點第一款第四目規定，新增檢核項目十五。

十五、配合修正第五點第二款第十二目及刪除同點第五款第九目，原檢核項目十四項次刪除，部分移列至項目十六。

十六、原檢核項目十五項次順移至項目十七；配合修正規定第七點內容修正文字。

十七、配合刪除現行規定第五

6	管	配合各交換層主機 IP 位址之變動，更新交換主機 IP 位址清單，並據以修正防火牆白名單設定，同時通知各交換層機關。	□符合 □部分符合 □不符合 □不適用			管	址清單，並據以設定防火牆白名單，異動時同時通知各交換層機關。	□部分符合 □不符合 □不適用		點第六款，刪除原檢核項目十六規定。 十八、配合修正規定第五點第一款第五目規定新增檢核項目十八。 十九、配合修正規定第五點第一款第二目規定新增檢核項目十九。 二十、配合修正規定第五點第一款第六目規定新增檢核項目二十。 二十一、配合修正規定第五點第一款第七目規定新增檢核項目二十一。 二十二、配合修正規定第五點第二款第十三目及同點第三款第九目規定新增檢核項目二十二。 二十三、配合修正規定第五點第三款第八目規定新增檢核項目二十三。
	交	依據管理層通知之交換主機 IP 位址清單進行防火牆白名單設定，如有交換主機 IP 位址異動需求，應通知管理層辦理連線異動事宜。				交	依據管理層通知之交換主機 IP 位址清單及所屬各終端層主機 IP 位址，進行防火牆白名單設定。			
7	交	交換層機關應以防火牆白名單控管機關層及網頁版公文收發模組用戶連線作業，並以一對一固定 IP 位址為原則，如機關層及網頁版公文收發模組用戶有 IP 位址異動需求，應通知交換層辦理連線異動事宜；確有一對多或非固定 IP 位址之需求者，應向交換層機關申請核准，並應建立 IP 位址與機關(構)名稱對照表，以	□符合 □部分符合 □不符合 □不適用		7	管 交	具有防範公文電子交換主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。	□符合 □部分符合 □不符合 □不適用		
					8	管 交	安裝防毒軟體，並定期更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。	□符合 □部分符合 □不符合 □不適用		
					9	交	當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並中止該公文之發送，避免惡意程式蔓延，並追查惡意程式來源，通知來源機關(單位)儘速處理惡意程式。如發生資安事件時，應	□符合 □部分符合 □不符合 □不適用		

		供追蹤及查檢之用。		
8	管 交	具有防範公文電子交換主機之目錄、檔案等遭受入侵及竄改之機制，並具備通報警告之能力。	□符合 □部分符合 □不符合 □不適用	
9	管 交	主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。	□符合 □部分符合 □不符合 □不適用	
10	管 交	當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並暫停相關主機服務，避免惡意程式蔓延，並追查惡意程式來源，通知來源機關（構）儘速處理惡意程式。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。	□符合 □部分符合 □不符合 □不適用	
11	管	訂定本系統安全傳輸協定，確保傳遞過程全程加密，並建立收發文確認機	□符合 □部分符合 □不符合	

		儘速通知管理層，並採取必要之因應控管措施。		
10	管	訂定本系統安全傳輸協定，確保傳遞過程全程加密，並建立收發文確認機制，防止未經授權之資料存取及竄改。	□符合 □部分符合 □不符合 □不適用	
11	管 交	定期辦理網頁及主機弱點掃描，並就掃描結果予以修補，且同時更新交換層及終端層相關程式。 定期進行網頁及主機弱點掃描，並將掃描結果提供管理層研析。	□符合 □部分符合 □不符合 □不適用	
12	管	定期辦理原碼檢測及滲透測試，或定期辦理資訊安全健檢，以預防或發現未知之威脅或攻擊。	□符合 □部分符合 □不符合 □不適用	
13	管	系統開發與維運工程師每年至少接受六小時安全程式撰寫技術及駭客攻擊手法攻防等資訊安全課程。	□符合 □部分符合 □不符合 □不適用	

		制,防止未經授權之資料存取及竄改。	□不適用	
12	管	定期進行本系統網頁及主機弱點掃描,並就掃描結果予以修補,且同時更新交換層及機關層相關程式。	□符合 □部分符合 □不符合 □不適用	
	交	定期進行本系統之網頁及主機弱點掃描,並將掃描結果提供管理層研析。		
13	管	定期辦理原碼檢測及滲透測試,或定期辦理資訊安全健檢,並進行必要之修補作業,以預防或發現未知之威脅或攻擊。	□符合 □部分符合 □不符合 □不適用	
14	管	系統開發與維運工程師每年至少接受六小時安全程式撰寫技術及駭客攻擊手法攻防等資訊安全課程。	□符合 □部分符合 □不符合 □不適用	
15	管	應檢查主機安裝之伺服器應用軟體憑證效期,並於憑證效期過期前更新憑證,避免交換異常。	□符合 □部分符合 □不符合 □不適用	
	交			

14	管	每年辦理之公文電子交換系統管理維護教育訓練應有三分之一課程時數為資訊安全(含個人資料保護)議題。	□符合 □部分符合 □不符合 □不適用	
	交	各機關負責公文收發之人員每年應接受至少一小時之公文電子交換系統資訊安全相關教育訓練課程。		
15	管	應將公文電子交換系統納入 ISMS 第三方認證範圍與資安監控中心(SOC)監控範圍防護。	□符合 □部分符合 □不符合 □不適用	
	交			
16	管	應使用檔案局發交之密碼模組辦理公文電子交換作業，且須負妥善管理之責任。	□符合 □部分符合 □不符合 □不適用	
	交			
		總結：		

以「管」、「交」分別標記為管理層及交換層之檢核項目

16	管	每年辦理之公文電子交換系統管理維護教育訓練應包含資訊安全(含個人資料保護)議題。	□符合 □部分符合 □不符合 □不適用		自評機關： 承辦人：　　聯絡電話：　　email: 單位主管：　　聯絡電話：　　email: 填表日期：	
17	管 交	應將公文電子交換系統納入ISMS第三方認證範圍與資安監控中心(SOC)監控範圍防護，SOC監控範圍須包含主機及應用系統日誌（log）監控。 自管中心須將日誌傳送管理層，以強化聯防機制，如自管中心為實體隔離環境，則須依管理層提供之監控規則進行布署設定。	□符合 □部分符合 □不符合 □不適用			
18	管 交	應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。	□符合 □部分符合□不符合 □不適用			
19	管 交	主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時	□符合 □部分符合□不符合 □不適用			

		應限縮存取權限,以杜絕任何可能之入侵管道。		
20	管 交	應使用並妥善保管管理層發交之密碼模組Ⅰ辦理公文電子交換作業。	□符合 □部分符合□不符合 □不適用	
21	管 交	本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。	□符合 □部分符合□不符合 □不適用	
22	管 交	至少應依資通安全責任等級分級辦法附表十所定資通系統防護基準中級以上之控制措施辦理本系統維護作業,委外作業應依資通安全管理法施行細則第四條規定事項辦理。	□符合 □部分符合□不符合 □不適用	
23	交	交換層機關提供網頁版公文收發模組介接使用本系統,應依本規範之要求辦理管理作業。	□符合 □部分符合□不符合 □不適用	
		總結：		

以「管」、「交」分別標記為管理層及交換層之檢核項目

<table>
<tr>
<td>自評機關：
承辦人：　　聯絡電話：　　email:
單位主管：　　聯絡電話：　　email:
填表日期：</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>附錄二 天元模組遺失毀損報告單
<table>
<tr><td colspan="5">天元模組遺失毀損報告單　報告時間：　年　月　日</td></tr>
<tr><td>單 位</td><td>職 稱</td><td>姓 名</td><td>出生年月日</td><td>身 分 證 字 號</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">遺失或毀損時間</td><td colspan="2">遺 失 或 毀 損 地 點</td></tr>
<tr><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="5">遺失或毀損之詳細經過遺失或毀損之詳細經過（請以條述式敘明，本欄位如不敷使用，請自行延伸）：</td></tr>
</table></td>
<td>一、附錄二刪除。
二、配合第五點修正規定。</td>
</tr>
</table>

	報告人簽章： 佐證人姓名 / 佐證人與使用人關係 國家發展委員會檔案管理局附註意見 ※本表係密件，請依文書處理手冊規定辦理一般公務機密文書處理及傳遞。	

附錄二　公文電子交換系統(交換層對機關層)資訊安全稽核彙整表

□定期稽核：稽核日期：　　稽核機關(構)數：

稽核比例：□全面性 □抽檢　%

□專案稽核：稽核日期：　　稽核機關(構)數：

稽核比例：□全面性 □抽檢　%

專案稽核原因：

編號	檢核項目	符合數目	部分符合數目	不符合數目	不適用數目	相關佐證說明
1	主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。					
2	定期進行本系統之網頁及主機弱點掃描，並將掃描結果提供管理層研析。					

一、附錄二新增。

二、配合修正規定第九點，訂定公文電子交換系統(交換層對機關層)資訊安全稽核彙整表。

3	當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並暫停相關主機服務，避免惡意程式蔓延至其他交換層及機關層，並追查惡意程式來源，通知來源機關(構)儘速處理惡意程式。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。							
4	應檢查主機安裝之伺服器應用軟體憑證效期，並於憑證效期過期前更新憑證，避免交換異常。							
5	應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。							
6	於接獲本系統更版通知，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。							

7	機關層主機應專機專用並採用固定 IP 位址，因特殊理由未能遵行者，應採取必要的監管措施，並提報交換層機關核准。如有主機 IP 位址異動需求，亦應通知交換層機關以進行白名單之設定。							
8	主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。							
9	應使用並妥善保管管理層發交之密碼模組Ⅰ辦理公文電子交換作業。							
10	本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。							
11	依循作業環境標準組態列表進行設定。							

<table>
<tr>
<td>總結：

稽核機關：
承辦人：　聯絡電話：　email:
單位主管：　聯絡電話：　email:
填表日期：
備註：必要時得檢附個別機關之稽核結果。</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>附錄三 天元模組緊急狀況處置報告單
<table>
<tr><td colspan="5">天元模組緊急狀況處置報告單　報告時間：　年　月　日</td></tr>
<tr><td>單位</td><td>職稱</td><td>姓名</td><td>出生年月日</td><td>身分證字號</td></tr>
</table></td>
<td>一、附錄三刪除。
二、配合第五點刪除原第六款規定。</td>
</tr>
</table>

緊急狀況發生時間			緊急狀況發生地點	
緊急狀況之詳細經過（請以條述式敘明，本欄位如不敷使用，請自行延伸）：				
				報告人簽章：
佐證人姓名			佐證人與使用人關係	

	佐證照片浮貼處 （得檢附電子檔圖片） 國家發展委員會檔案管理局附註意見 ※本表係密件，請依文書處理手冊規定辦理一般公務機密文書處理及傳遞。	
附錄三　公文電子交換系統(交換層對終端層)資訊安全稽核彙整表 □定期稽核：稽核日期：　　稽核機關(構)數： 稽核比例：□全面性 □抽檢　% □專案稽核：稽核日期：　　稽核機關(構)數： 稽核比例：□全面性 □抽檢　% 專案稽核原因：	**附錄五 公文電子交換系統(交換層對終端層)資訊安全稽核彙整表** □定期稽核：稽核日期：　　稽核機關數： 稽核比例：□全面性 □抽檢　% □專案稽核：稽核日期：　　稽核機關數： 稽核比例：□全面性 □抽檢　% 專案稽核原因：	一、附錄序號變更，現行附錄五變更為附錄三。 二、配合修正規定第五點第一款第一目規定整併檢核項目二內容，修正文字。 三、配合修正規定第五點第一款第一目規定，原檢核項目二整併至檢核項目一，爰刪除。 四、原檢核項目三配合修正規

編號	檢核項目	符合數目	部分符合數目	不符合數目	不適用數目	相關佐證說明
1	主機應安裝防毒軟體及定期進行漏洞修補、更新病毒碼及掃描電腦主機，偵測有無感染電腦病毒。					
2	機關(構)如有資訊異動(例如機關(構)代碼、機關(構)名稱、電子憑證IC卡等)或機關(構)裁撤情形，應依管理層發布之程序辦理連線異動事宜。					
3	應落實本系統主機系統校時機制，確保系統公文交換時間資訊正確一致。					
4	系統登錄註冊之電子憑證IC卡應專卡專用，並指定專人保管，未使用時應上鎖收存以防止遺失，並					

編號	檢核項目	符合數目	部分符合數目	不符合數目	不適用數目	相關佐證說明
1	作業系統應定期進行漏洞修補。					
2	安裝防毒軟體，並定期更新病毒碼，對於收發公文及其附件進行掃描，偵測有無感染電腦病毒。					
3	於接獲本系統更新版通知後，進行程式檢核碼驗證，確認未遭竄改後，儘速完成系統更新。					
4	主機應專機專用並採用固定IP位址，因特殊理由未能專機專用者，應採取必要的監管措施，並提報上級主管機關備查。					
5	機關(單位)如有資訊異動(例如IP位址、機關代碼、機關名稱、機關憑證、機關地址等)或機					

定刪除現行規定第五點第三款第三目規定刪除。

五、原檢核項目四配合修正規定刪除現行規定第五點第三款第四目規定刪除。

六、原檢核項目五項次順移至項目二；配合修正規定第五點第五款第一目規定修正文字。

七、配合修正規定第五點第一款第五目規定新增檢核項目三。

八、原檢核項目六項次順移至項目五，酌修文字。

九、原檢核項目七配合修正規定刪除現行規定第五點第三款第七目規定刪除。

十、原檢核項目八項次順移至項目四；配合修正規定第五點第一款第四目規定，新增憑證效期維護規定文字。

	於憑證效期過期前更新憑證IC卡，避免交換異常。					
5	主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。					
6	當偵測到惡意程式等警訊時，應對惡意程式先行阻絕，並暫停相關主機服務，避免惡意程式蔓延，並追查惡意程式來源，通知來源機關(構)儘速處理惡意程式。如發生資安事件時，應依相關辦法辦理事件通報，並副知管理層及採取必要之因應控管措施。					
7	應使用並妥善保管管理層發交之密碼模組Ⅰ辦理公文電子交換作業。					

	關裁撤情形，應填寫連線異動申請表辦理連線異動事宜。					
6	終端層主機應禁止安裝點對點(P2P)、即時通訊(IM)、社交軟體或來源不明之網路應用程式，使用網路芳鄰時應限縮存取權限，以杜絕任何可能之入侵管道。					
7	使用機關(單位)每半年應至少執行備份或封存作業一次，以確保個人電腦系統安全。					

十一、原檢核項目九配合現行第五點第三款第九目修正刪除。

十二、原檢核項目十配合修正規定刪除現行規定第五點第六款規定刪除。

十三、配合修正規定第五點第一款第三目規定新增檢核項目六。

十四、配合修正規定第五點第一款第六目規定新增檢核項目七。

十五、配合修正規定第五點第一款第七目規定新增檢核項目八。

8	本系統應納入各機關(構)執行政府組態基準(GCB)導入範圍。					

總結：

稽核機關：

承辦人：　　聯絡電話：　　email:

單位主管：　　聯絡電話：　　email:

填表日期：

備註：必要時得檢附個別機關之稽核結果。

8	系統登錄註冊之電子憑證 IC 卡應專卡專用，並指定專人保管，未使用時應上鎖收存以防止遺失。					
9	各機關負責公文收發之人員每年應接受至少一小時之公文電子交換系統資訊安全相關教育訓練課程。					

	10	應使用檔案局發交之密碼模組辦理公文電子交換作業，且須負妥善管理之責任。					

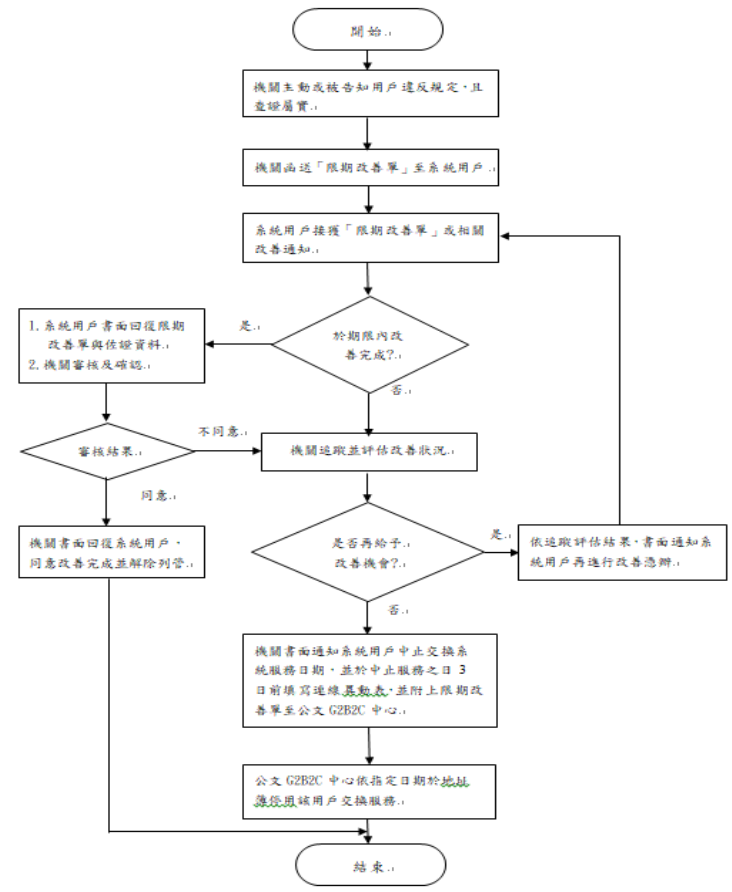
總結：

稽核機關：

承辦人：　聯絡電話：　email:

單位主管：　聯絡電話：　email:

填表日期：

	備註：必要時得檢附個別機關之稽核結果。	
附錄四　公文電子交換系統用戶中止服務流程 **附錄四　公文電子交換系統用戶中止服務流程**  **※本流程之書面回復，得以正式公函、傳真或電子郵件方式為之。**		一、附錄四新增。 二、配合第十三點修正規定，新增公文電子交換系統用戶中止服務流程。