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

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) 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。

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。

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，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。

貳、機關權責

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) 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。

(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。
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。

(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相關教育訓練課程。

(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。

(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。

(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，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。

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。

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。

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。

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。

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。

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。

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。

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																	
傳真電話																	

機關全銜				
地址				
聯絡人		聯絡電話		
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				
新機關名稱				
☐更換機關憑證	憑證卡類別	☐GCA　☐XCA　☐MOEACA		
	憑證卡號		啟用日期	年月日
	憑證卡用途	☐收發合一	☐發文憑證　☐收文憑證	

製表單位：公文 G2B2C 資訊服務中心
客服專線：(02)2503-0030　下載網址：www.good.nat.gov.tw

公文 G2B2C 資訊服務中心

連線異動申請表

申請機關章	備註

以下部分請勿填寫，由客服人員填寫

客服處理情形說明

國家發展委員會檔案管理局審核		審核日期	
公文中心審核		中心處理人員	

※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

附錄二　天元模組遺失毀損報告單

天元模組遺失毀損報告單				
報告時間：　年　月　日				
單　位	職　稱	姓　名	出生年月日	身分證字號
遺失或毀損時間			遺失或毀損地點	
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）：				
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。

附錄三　天元模組緊急狀況處置報告單

天元模組緊急狀況處置報告單				
報告時間：　年　月　日				
單位	職稱	姓名	出生年月日	身分證字號
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。

附錄四　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。	□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。		
7	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			
8	管	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	
	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
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，應儘速通知管理層，並採取必要之因應控管措施。	□符合 □部分符合 □不符合 □不適用	
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	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。	□符合 □部分符合 □不符合 □不適用	
	交	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。		
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	
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：		

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：

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。					
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。					

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
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。