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　　%

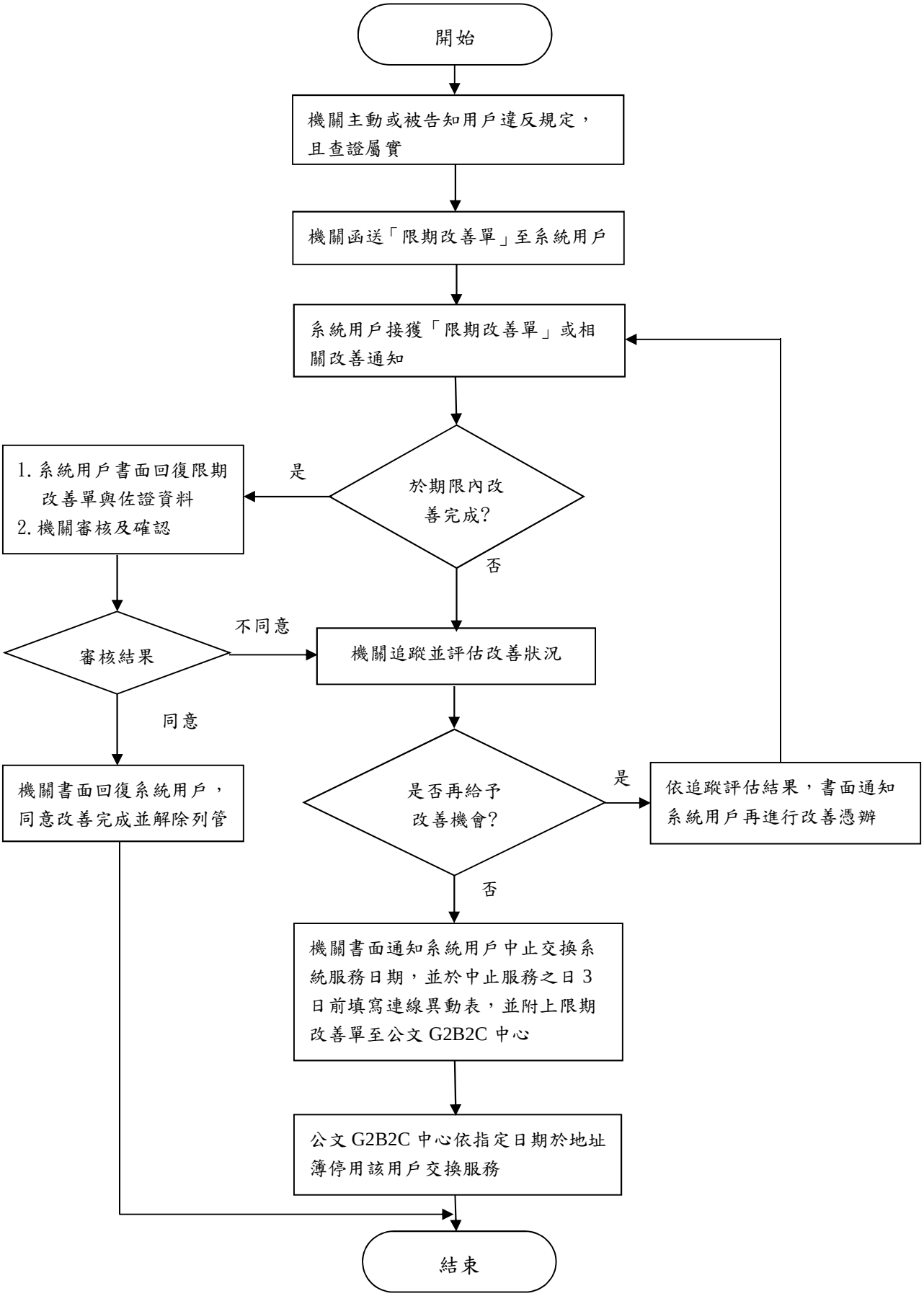
專案稽核原因：

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。