

應用戶役政資訊系統安全稽核要點

102年2月5日台內戶字第1020091635號函訂定

105年5月13日台內戶字第1051201718號函修正

111年7月5日台內戶字第1110242502號函修正

112年5月10日台內戶字第1120241543號函修正

112年9月8日台內戶字第1120243620號函修正，並自113年1月1日生效

一、為促使各機關應用戶役政資訊系統符合內政部（以下簡稱本部）訂定之相關資訊安全管理規定，並依個人資料保護法規定，落實資訊安全管理及個人資料保護，特訂定本要點。

二、本要點之主管機關：在中央為本部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

各級主管機關應分別組成稽核小組，依本要點執行稽核作業。

三、稽核小組之組成及任務：

（一）戶政：

1. 本部之稽核小組由本部戶政司、資訊服務司及政風處組成，執行直轄市、縣（市）政府、鄉（鎮、市、區）之戶政機關、本部連結機關、資料持有、使用機關及戶役政資訊系統委外廠商之外部稽核作業。對持有全國性資料之連結機關，得洽請資訊安全專業機關（構），會同執行外部稽核作業。

2. 直轄市、縣（市）主管機關（以下簡稱地方主管機關）之稽核小組由直轄市、縣（市）民政局（處）召集相關單位組成，執行所屬戶政事務所、連結機關及涉戶政資訊系統作業相關委辦機關或委外廠商之外部稽核作業。

（二）役政：

1. 本部之稽核小組由本部役政司、替代役訓練及管理中心等相關單位組成，執行直轄市、縣（市）政府、鄉（鎮、市、區）之役政機關及本部連結機關之外部稽核作業。

2. 地方主管機關之稽核小組由直轄市、縣（市）役政單位召集相關單位組成，執行所轄公所、連結機關及涉役政資訊系統作業相關委辦機關或委外廠商之外部稽核作業。

四、各級戶役政機關、連結機關及涉戶役政資訊系統作業相關之委辦機關或委

外廠商，應分別指定專人或成立稽核小組，執行內部稽核作業。

五、稽核頻率：

(一)內部稽核：

各級戶役政機關、連結機關、資料持有、使用機關及涉戶役政資訊系統作業相關之委辦機關或委外廠商，每半年至少辦理一次。

(二)外部稽核：

1. 本部對持有全國性戶役政資料連結機關、地方主管機關及戶役政資訊系統委外廠商，每年至少辦理一次外部稽核，對其他連結機關每五年至少辦理一次。
2. 地方主管機關對所屬戶政事務所、所轄鄉（鎮、市、區）公所、連結機關及涉戶役政資訊系統作業相關之委辦機關或委外廠商，每年至少辦理一次。
3. 中央及直轄市、縣（市）各連結機關對資料持有、使用機關及涉戶役政資訊系統作業相關之委辦機關或委外廠商，每半年至少辦理一次。

六、稽核重點：

- (一)對各級戶役政機關之稽核包括資產管理、人力資源、人員安全管制、通訊與作業管理、存取控制、資訊安全事故管理、遵循性及其他事項。
- (二)對連結機關之稽核包括人力資源、人員安全管制、帳號密碼管理、資料管理機制、線上資料查詢、檔案傳輸、內部及外部稽核落實情形、資通安全教育訓練及其他事項。
- (三)對委辦機關或委外廠商之稽核包括人力資源、人員安全管制、實體與環境安全、通訊與作業管理、存取控制、資訊安全事故管理及契約文件各項資訊安全相關規定。
- (四)各級戶役政機關應將使用外機關查詢系統納入稽核範圍。

七、內部稽核程序及稽核結果追蹤處理，依下列程序或機關資訊安全管理系統相關規範辦理：

- (一)召開起始會議或簽報主管訂定稽核日期並通知稽核及受稽核人員，簽報內容應包含稽核目的、範圍及程序等相關資訊。
- (二)召開結束會議或提出稽核結果報告簽報主管核閱，稽核結果報告應妥為保管，保存年限五年。
- (三)稽核結果如有不符合事項，應追蹤受稽核單位矯正執行時效及有效性。

(四)每次稽核前應對前次稽核不符合事項及改善情形進行複核。

八、本部對地方主管機關稽核程序及稽核結果追蹤處理：

(一)排定至各直轄市、縣(市)政府及擇定其所屬戶政事務所、所轄鄉(鎮、市、區)公所稽核之時程，並函知各直轄市、縣(市)政府。

(二)以實地訪談、觀察與抽查紀錄及表單方式進行稽核為原則。但遇有特殊情況者，得以書面結合視訊方式為之。受稽核機關應配合提供相關資料。

(三)完成稽核作業後，應將稽核結果、說明及應改善事項詳實記錄於稽核紀錄表(附件一)，經受稽核機關確認簽章。

(四)直轄市、縣(市)政府受稽核結果，如有不符合事項，應依稽核結果及應改善事項進行改善，並於受稽核日次一工作日起七日內提出改善措施及預定完成日期，填列於改善措施紀錄單(附件二)，經主管簽章後，函送本部，並於預定完成期限內執行改善完畢後，檢附相關證明文件函送本部辦理書面複核。

(五)戶政事務所、鄉(鎮、市、區)公所受稽核結果，如有不符合事項，應依稽核結果及應改善事項進行改善，並於受稽核日次一工作日起七日內提出改善措施及預定完成日期，填列於改善措施紀錄單，經主管簽章後，函送直轄市、縣(市)政府，並於預定完成期限內改善完畢後，檢附相關文件函送直轄市、縣(市)政府；直轄市、縣(市)政府應於文到次日起一個月內實地辦理複核，並於改善措施紀錄單填列複核結果，函送本部備查。

九、本部對連結機關稽核程序及稽核結果追蹤處理：

(一)擇定受稽核機關並排定稽核行程，申請全國性戶役政資料之連結機關原則全數納入稽核，其他連結機關稽核擇定原則包括但不限於下列各款：

1. 近二年使用戶役政資訊之資料量較多者。
2. 近二年曾經不當使用戶役政資訊者或查有資料未銷毀情事者。
3. 近三年曾受稽核，稽核結果不符合事項較多，或應改善事項尚未完成者。
4. 近五年未曾接受稽核者。
5. 查有承辦人員、專責人員或單位主管異動未通知本部者。

- (二)函知受稽核機關稽核時程。受稽核機關應先自評並填寫連結機關應用戶役政資訊連結作業稽核自我評審表（附件三），依期限函復。
- (三)進行實地稽核，受稽核機關應配合提供相關資料。但相關資料屬受稽核機關應保守之秘密或有其他法定原因者，不在此限。完成稽核作業後，應將稽核結果、說明及應改善事項詳實記錄於稽核紀錄表（附件四）。
- (四)將稽核結果函知受稽核機關。稽核結果如有不符合事項，受稽核機關應於受稽核結果通知後三十日內提出改善報告，內容應包含改善期限、改善方式及列管作為，並依改善報告內容函復改善情形。屆期未提出或未改善者，應停止連結提供資料。
- (五)稽核發現缺失涉及戶政資料嚴重外洩者，責受稽核機關依資通安全事件通報及應變辦法規定之程序辦理。
- (六)定期追蹤受稽核機關改善情形，追蹤處理程序如下：

- 1. 將當年稽核結果之不符合事項，填列稽核結果及改善情形追蹤表（附件五）。
- 2. 每半年查證受稽核機關應改善事項完成情形，受稽核機關完成全部應改善事項，始解除追蹤列管。

- (七)完成稽核作業後，如有發生其他缺失情形，受稽核機關仍應限期提出改善報告。屆期未提出或未改善者，應停止連結提供資料。

十、地方主管機關對所屬戶政事務所或所轄鄉（鎮、市、區）公所稽核程序及稽核結果追蹤處理：

- (一)擇定所屬戶政事務所、所轄鄉（鎮、市、區）公所辦理稽核，並函知稽核時程。
- (二)以實地訪談、觀察與抽查紀錄及表單方式進行稽核為原則。但遇有特殊情況者，得以書面結合視訊方式為之。受稽核之戶政事務所、鄉（鎮、市、區）公所應配合提供相關資料。
- (三)完成稽核作業後，應將稽核結果、說明及應改善事項詳實記錄於稽核紀錄表（附件一），經受稽核之戶政事務所、鄉（鎮、市、區）公所確認簽章。
- (四)受稽核之戶政事務所、鄉（鎮、市、區）公所如有不符合事項，應依稽核結果及應改善事項進行改善，並於受稽核日次一工作日起七日內

提出改善措施及預定完成日期，填列於改善措施紀錄單（附件二），經主管簽章後，函送地方主管機關，並於預定完成期限內執行改善完畢後，檢附相關文件函送地方主管機關辦理書面複核。

十一、地方主管機關對連結機關稽核程序及稽核結果追蹤處理：

（一）每年擇定連結機關辦理稽核，擇定原則包括但不限於下列各款：

1. 近二年使用戶役政資訊之資料量較多者。
2. 近二年曾經不當使用戶役政資訊者或查有資料未銷毀情事者。
3. 近三年曾受稽核，稽核結果不符合事項較多，或應改善事項尚未完成者。
4. 近五年未曾接受稽核者。
5. 查有承辦人員、專責人員或單位主管異動未通知地方主管機關者。

（二）函知受稽核機關稽核時程。受稽核機關應先自評並填寫連結機關應用戶役政資訊連結作業稽核自我評審表（附件三），依期限函復。

（三）進行實地稽核，受稽核機關應配合提供相關資料。但相關資料屬受稽核機關應保守之秘密或有其他法定原因者，不在此限。完成稽核作業後，應將稽核結果、說明及應改善事項詳實記錄於稽核紀錄表（附件四）。

（四）將稽核結果函知受稽核機關。稽核結果如有不符合事項，受稽核機關應於受稽核結果通知後三十日內提出改善報告，內容應包含改善期限、改善方式及列管作為，並依改善報告內容函復改善情形。

（五）定期追蹤受稽核機關改善情形，追蹤處理程序如下：

1. 將當年稽核結果之不符合事項，填列稽核結果及改善情形追蹤表（附件五）。
2. 每半年查證受稽核機關應改善事項完成情形，受稽核機關完成全部改善事項，始解除追蹤列管。

十二、本部及地方主管機關對涉戶役政資訊系統作業相關之委辦機關或委外廠商稽核程序及稽核結果追蹤處理：

（一）函知受稽核機關或廠商稽核時程。

（二）進行實地稽核，受稽核機關或廠商應配合提供相關資料。

（三）完成稽核作業後，應將稽核結果、說明及應改善事項詳實記錄於稽核紀錄表。

(四)將稽核結果函知受稽核機關或廠商。稽核結果如有不符合事項，受稽核機關或廠商應於受稽核結果通知後三十日內將具體改進措施函復稽核機關。

(五)將稽核結果之不符合事項，填列稽核結果及改善情形追蹤表（附件五），待受稽核機關或廠商完成全部改善事項，始解除追蹤列管。

十三、中央及直轄市、縣（市）各連結機關對資料持有、使用機關及涉戶役政資訊系統作業相關之委辦機關或委外廠商，稽核程序及稽核結果追蹤處理，由各連結機關定之。

十四、本要點應配合相關資訊安全管理規定及稽核結果進行修正調整，以確保稽核作業流程及稽核項目符合實務情形，原則每二年進行修正一次，如遇有特殊情形可即時進行修正。