抄件

檔　　號：
保存年限：

交通部政風處　函

機關地址：10052臺北市仁愛路1段50號
傳真：(02)2331-7345
聯絡人：黃國聖
聯絡電話：(02)2349-2545
電子郵件：huangks@motc.gov.tw

受文者：

發文日期：中華民國108年2月26日
發文字號：政字第1080900419號
速別：普通件
密等及解密條件或保密期限：
附件：如主旨

裝

主旨：檢送「政風機構協助機關（構）推動資訊使用管理稽核實施計畫」及「政風機構協助機關（構）推動資訊使用管理稽核項目表（參考範本）」各1件，請查照並轉知所屬辦理。

訂

說明：

一、依據法務部廉政署108年2月23日廉政字第10807003420號書函辦理。

二、為協助各機關(構)強化資通安全管理機制，防範公務機密外洩，確保資料、系統、設備及網路安全，法務部廉政署爰訂定旨揭計畫。請各政風機構以協助機關（構）推動資訊使用管理稽核為重點，協調各機關（構）資訊及業務單位建置使用者紀錄檔、界定系統存取異常狀況及建構相關通報機制，俾有效防範公務機密外洩，落實公務機密維護。

線

三、旨揭稽核項目表屬參考範本，各政風機構得視機關（構）實際狀況增刪稽核項目，並結合各機關（構）現有之資通安全稽核表併同辦理。

正本：中華郵政股份有限公司政風處、交通部公路總局政風室、交通部臺灣鐵路管理局政風室、臺灣港務股份有限公司政風處、交通部高速公路局政風室、交通部民用

航空局政風室、交通部鐵道局政風室、交通部航港局政風室、交通部中央氣象局政風室、桃園國際機場股份有限公司政風處、交通部觀光局政風室

副本：本處第一科

政風機構協助機關(構)推動資訊使用管理稽核實施計畫

壹、依據

一、政風機構人員設置管理條例第4條第7款。

二、政風機構人員設置管理條例施行細則第10條第3款。

三、行政院及所屬各機關資訊安全管理要點第9點第1項第3款規定。

四、政風機構維護公務機密作業要點第14點、第15點規定。

貳、目的

為協助各機關(構)強化資通安全管理機制，防範公務機密外洩，確保資料、系統、設備及網路安全，特訂定本計畫。

參、任務編組

由各政風機構結合機關(構)資訊單位按本機關(構)實際分工與職掌，辦理資訊使用管理稽核作業。

肆、稽核時機

結合各機關(構)依資通安全責任等級分級辦法規定之次數，辦理內部資通安全稽核。

伍、工作內容及要領

一、各政風機構協調各機關(構)資訊單位(或相關權管單位)建置使用者紀錄檔（Log File）

(一)系統應建置、啟動、處理及保留使用者紀錄檔(Log File)，如紀錄檔資料不足以作為稽核管理使用，得協調另行開發或購置進階之管理工具。

(二)系統查詢軌跡紀錄檔（Log）應處於啟動狀態，並應定期備份轉出檔案後保存，使其具有連貫性，以作為日後調查及監督之用。

(三)系統查詢軌跡紀錄檔（Log）應指定專人定期及日常檢視，並做成書面紀錄備查。

(四)應依規定確保使用者紀錄檔（Log File）之建置與保存，俾利查察違規使用、越權查閱、下載資訊等異常情事，並就資通安全漏洞研採補救與防範措施，以及追究相關法律或行政責任，以有效防止公務機密資訊外洩。

二、各政風機構協調各機關(構)資訊及業務單位，就機關(構)現有資通系統特性及運作現況，界定以下例示之「系統存取異常狀況」(請視機關實際需求適時增修)及建構相關通報機制，並協調資訊單位即時或按月彙送系統存取異常狀況報表供政風機構進行瞭解：

(一)系統登入：

例如系統登入(失敗)次數異常頻繁、於非勤務時間登入系統、登入系統連線之電腦設備網際網路協定(IP)位址異常、使用他人或離(休)職員工帳號登入等異常狀況。

(二)使用時間：

例如相較於一般使用習慣，單次使用系統時間或累計使用系統時間異常增加等情形。

(三)查詢異常：

例如查詢筆數異常頻繁、未於系統登載「案號」或「查詢事由」，亦未設置「電腦查詢資料登記簿」、「查詢內容」與登載之「案號」或「查詢事由」不

符、具系統存取特別權限者查詢筆數異常頻繁、以機關首長、時事名人或公眾人物之姓名為查詢條件等異常狀況。

(四)其他系統存取異常狀況

三、各政風機構應協調資訊單位加強資訊使用管理及內控機制，並加強資訊機密維護宣導，俾有效防範電腦犯罪與資訊機密外洩。

四、各政風機構衡酌本機關(構)資通系統特性、系統存取政策、系統存取異常狀況、授權規定及其他使用管理規定，協調資訊單位據以研（修）訂稽核項目(如附件參考範本)，並就機關(構)內部現有資通管理規定，建議將政風機構納入系統存取異常狀況之受通報單位。

五、協助辦理資訊使用管理稽核重點

(一)瞭解前揭系統存取狀況各項管制作為是否落實，及系統存取異常個案是否確實通報政風機構。

(二)退（離）職、職務異動及具特別存取權限等人員之權限之管理，檢視其申請或核准文件是否完整，及是否依規定取消或調整相關存取權限。

(三)委外廠商人員於系統存取權限、資通安全責任及保密規定等辦理情形。

陸、稽核結果處理

一、各項稽核未盡事宜、改善意見，於稽核後彙整簽報機關(構)首長或其授權人員，並將建議事項移請相關單位檢討改善或參處，另藉由機關安全維護會報或相關

會議，主動追蹤管考專案稽核所見缺失事項之改善情形。

二、發現重大事件恐肇生資安事件之虞者，簽報機關(構)首長或其授權人員核定後，追究相關責任，通知限期改善，並於機關安全維護會報或相關會議適時報告。

柒、行政支援事項

一、各政風機構協助辦理稽核作業得調閱有關資料、實地測試或檢查資訊軟、硬體設備使用情形，並請各受稽核單位相關人員提供說明。

二、受稽核單位、個人對於稽核人員實施稽核時，應充分配合執行。

政風機構協助機關(構)推動資訊使用管理稽核項目表(參考範本)-1080223發文版

(以下為例示項目，得結合機關資通安全稽核項目辦理)

項次	項目名稱	查核結果	查核情形(簡述符合、部分符合、不符合或不適用之原因)	紀錄文件	處理情形或改善措施
1	**系統查詢軌跡紀錄檔(Log)：**				
1-1	資訊單位是否有建立及啟動系統查詢軌跡紀錄檔(Log)，並保存一段時間(保存多久？)，以作為日後調查及監督之用。	□符合 □不符合 □部分符合 □不適用			
1-2	資訊單位系統紀錄檔，是否有定期備份轉出檔案後保存。	□符合 □不符合 □部分符合 □不適用			
1-3	資訊單位是否有專人隨時(經常)檢視。	□符合 □不符合 □部分符合 □不適用			
2	**系統存取異常狀況情形：**				
2-1	系統登入次數是否正常(相較一般使用習慣，系統登入次數小於____次)。	□符合 □不符合 □部分符合 □不適用			
2-2	系統登入失敗次數是否正常(相較一般使用習慣，連續失敗次數小於____次)。	□符合 □不符合 □部分符合 □不適用			
2-3	登入系統查詢時段是否正異常(例如於正常勤務時間登入系統)。	□符合 □不符合 □部分符合 □不適用			
2-4	使用者系統連線電腦設備網際網路協定(IP)位址，是否正常(例如IP 位址為使用者公務慣用之位址)。	□符合 □不符合 □部分符合 □不適用			
2-5	使用者之帳號密碼是否沒有共用或交由他人使用情形。	□符合 □不符合 □部分符合 □不適用			
2-6	是否沒有以離(休)職員工帳號登入使用之情形。	□符合 □不符合 □部分符合 □不適用			
2-7	單次使用系統時間是否無正常(相較一般使用習慣，單次使用系統時間小於____小時)。	□符合 □不符合 □部分符合 □不適用			

項次	項目名稱	查核結果	查核情形(簡述符合、部分符合、不符合或不適用之原因)	紀錄文件	處理情形或改善措施
2-8	累計使用系統時間是否正常(相較一般使用習慣，每月使用系統累計時間小於____小時)。	□符合 □不符合 □部分符合 □不適用			
2-9	使用者查詢筆數是否正常(相較一般使用習慣，每月查詢筆數小於____筆)。	□符合 □不符合 □部分符合 □不適用			
2-10	使用者是否依規定於查詢系統登載「案號」或「查詢事由」。	□符合 □不符合 □部分符合 □不適用			
2-11	系統雖無法登載「案號」或「查詢事由」，是否另設置「電腦查詢資料登記簿」管制使用情形。	□符合 □不符合 □部分符合 □不適用			
2-12	使用者「查詢內容」與登載之「案號」(如收文號)或「查詢事由」是否相符。	□符合 □不符合 □部分符合 □不適用			
2-13	系統存取特別權限者查詢筆數是否正常(例如每月查詢筆數小於____筆)。	□符合 □不符合 □部分符合 □不適用			
2-14	是否沒有以機關首長、時事名人或公眾人物之姓名為查詢條件情事（亦即確認查詢作業係基於公務需要)。	□符合 □不符合 □部分符合 □不適用			
2-15	是否有指派專人定期查核機關內使用者正常查詢機敏性資料系統，並留存查核紀錄備查。	□符合 □不符合 □部分符合 □不適用			
3	**系統存取異常狀況通報情形：**				
3-1	是否符合機關需求界定或修訂系統存取異常狀況。	□符合 □不符合 □部分符合 □不適用			
3-2	是否建立系統存取異常狀況通報機制且定期通報政風單位。	□符合 □不符合 □部分符合 □不適用			