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。