政府機關（構）資安事件數位證據保全標準作業程序

一、訂定目的

為使各級政府機關（構）於執行資安事件調查時能有效保全及運用數位證據，及執行人員於執行數位證據識別、蒐集、擷取、封緘及運送作業時有所依循，爰參考相關數位鑑識國際標準(ISO/IEC 27037 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence，數位證據識別、蒐集、擷取及保存指引)，特訂定本作業程序。

二、適用機關

各級政府機關（構)(以下簡稱各機關)。

三、適用時機

各機關基於資安事件之調查，需進行電腦系統之數位證據識別、蒐集、擷取、封緘及運送作業時，適用本作業程序。

四、人員職掌

（一）數位證據保全人員

執行數位證據識別、蒐集、擷取、封緘及運送作業。

（二）記錄人員

１、視現場狀況，於數位證據保全人員執行數位證據識別、蒐集、擷取及封緘作業過程中，以錄影、拍照及其他方式記錄資安事件現場。

２、協助資安事件調查現場之秩序維持。

五、名詞定義

（一）揮發性資料

指電腦系統中，若拔除電源或關機後，即會消逝之資料內容。

（二）邏輯性資料

指得於目前作業系統中之檔案系統所存取之檔案資料。

（三）數位證據

指經解釋後得為事實佐證之數位資料。

（四）數位證物

指儲存數位證據之實體設備。

（五）證據監管鏈要求

指數位證據識別、蒐集、擷取、封緘及運送作業過程中，應確保證據完整性與一致性，避免數位證據遭受竄改等不當行為之發生。

（六）電腦系統

包括下列裝置：

１、電腦、周邊設備及數位儲存媒體。

２、網路連線設備。

３、監視錄影系統。

４、其他能儲存數位資料之裝置。

六、數位證據保全標準作業程序

（一）數位證據識別

１、維護現場完整

（１）記錄人員應要求在場人員停止操作作業，如電腦系統處於開機情況下，為避免改變數位證據原始狀態，原則上不關機。但若情況特殊，得依現場狀況審酌。電腦系統於關機情況下之數位證據保全作業程序，依六、（二）電腦設備或儲存媒體蒐集之步驟辦理。

（２）記錄人員應協助資安事件現場秩序之維持，針對資安事件之系統設備週遭附近人員進行現場疏導作業，以隔離在場人員與數位證據之接觸，另應確保非業務承辦人員或未取得部門權責主管授權之人員不得進出資安事件現場。

２、判斷與案情相關之數位證物。

３、記錄現場現況

記錄人員視現場狀況以錄影、拍照或其他方式記錄現場，記錄時得考量運用靜態之照片或動態之影像：

（１）非必要情況下，勿觸碰或移動現場相關數位證物。

（２）記錄相關標的設備及其他數位證物之所在位置，如電腦系統及周邊設備、筆記型電腦及儲存媒體，拍照方式如下:

甲、電腦系統及周邊設備

應拍照電腦系統及周邊設備擺設位置、電腦主機正面、側面及背面之照片。

乙、筆記型電腦

應拍照筆記型電腦及周邊設備擺設位置、筆記型電腦上面、下面及側面之照片。

丙、光碟片、隨身碟、記憶卡及其他可攜式儲存媒體

應拍照光碟片、隨身碟、記憶卡及其他可攜式儲存媒體所擺設位置及儲存媒體正面照片，另應視儲存媒體類型，考量拍照二側面及背面照片。

（二）電腦設備或儲存媒體蒐集

1、如系統於得關機情況下，各機關原則上應封緘完整電腦設備，以待上級機關或鑑識單位進行後續協助。但如確有拆卸之必要者，記錄人員須針對儲存媒體拆卸及取出過程進行全程錄影，並應將儲存媒體進行封緘，並視需要運送至上級機關或鑑識單位。所稱上級機關，指該機關直屬之上一級機關；其無上級機關者，由該機關執行本作業程序所規定上級機關之職權。

2、如系統於得關機情況下，且有其他外接式儲存媒體存在時，數位證據保全人員應將儲存媒體進行封緘，並視需要運送至上級機關或鑑識單位。記錄人員須針對儲存媒體拆卸及取出過程進行全程錄影。如以拍照方式進行，其步驟如下：

（1）針對儲存媒體拆卸前進行拍照（包含線材連結畫面）。

（2）針對儲存媒體拆卸後進行拍照（包含線材無連結畫面）。

（3）針對儲存媒體取出時進行拍照。

3、如伺服主機系統無法中斷服務，應在上級機關或鑑識單位之監督下，以嚴謹之方式進行資料轉錄。

4、針對儲存媒體之廠牌、型號、序號及儲存容量等相關資訊進行拍照。數位證據保全人員應將其數位證據蒐集結果填寫於數位證據蒐集工作表（電腦設備）或數位證據蒐集工作表（儲存媒體）。

（三）揮發性與邏輯性資料擷取

1、各機關得視其資訊人力資源進行不同程度之揮發性及邏輯性資料擷取。

2、如相關標的設備處於開機狀態下，數位證據保全人員應考量資安事件類型及現場狀況後，擷取揮發性資料，以避免部分儲存於記憶體中之重要資料因系統關機而消逝。

3、數位證據保全人員應考量資安事件類型及現場狀況後，擷取邏輯性資料，如作業系統資訊、網路狀態、執行程序資訊、系統稽核日誌紀錄及使用者上網行為紀錄等。

4、針對防火牆設備、入侵偵測或防禦設備、紀錄保存與資安事件分析設備、防毒設備、流量控管或網路監控設備、應用系統及資料庫等設備，若各機關有資訊人力，得在數位證據保全人員檢視下，由應用系統或網路管理人員將稽核日誌檔案匯出至特定目錄內，由數位證據保全人員對其進行邏輯性資料擷取。

5、數位證據保全人員於擷取揮發性與邏輯性資料完畢後，應產生

相對應之雜湊運算值，並記錄擷取之資訊或以自動化工具所產生之報表為之，如擷取日期與時間、電腦名稱、所蒐集之揮發性與邏輯性資料項目、雜湊運算值等，經執行人員與資安事件發生單位主管簽章確認。

6、記錄人員應以全程錄影或拍照方式記錄揮發性與邏輯性資料擷取之步驟。如以拍照方式進行，其步驟如下：

（1）針對工具連結至標的設備時進行拍照。

（2）針對工具執行時之螢幕畫面進行拍照。

（3）針對工具之重要操作步驟之螢幕畫面進行拍照。

（4）針對工具執行完成時之螢幕畫面進行拍照。

7、數位證據保全人員應將揮發性與邏輯性資料進行封緘，並視需要運送至上級機關或鑑識單位。

（四）證據封緘作業

1、現場所蒐集之數位證據應確實清點，每一項數位證據應分別填寫一張證據監管鏈表，並固定至對應之證據收集容器或公文袋上。

2、數位證據於封緘前應妥善包裝並考量其保護措施，以避免靜電或運送過程中發生碰撞與震動等。

3、封緘完整電腦設備時，數位證據保全人員得考量將周邊設備、連接線材及電源線一併進行封緘。

4、數位證據保全人員應將數位證據、揮發性與邏輯性資料擷取紀錄及數位證據蒐集工作表等文件放置於證據收集容器或公文袋；其開口處應進行完整密封，並於所有接縫處由數位證據保全人員簽章及簽具日期時間。

5、記錄人員應於數位證據封緘過程中進行全程錄影。

6、數位證據保全人員於將數位證據攜出各機關前應填列證據取得清單，並交由在場相關人員簽章確認。所有工作（紀錄）表單及清單經查核無誤後，由資安事件發生單位影印留存。

7、封緘之設備應避免放置於鄰近強光、高溫、潮溼、磁場及灰塵之場所。

（五）證據運送作業

1、證據運送過程中皆應全程進行監看作業，並應遠離磁場、高溫或直接日照強光熱源下，及避免遭受液體潑灑、重大衝擊與震動。

2、證據運送過程中應符合證據監管鏈要求，無被竄改等不當行為

發生之可能性，並於每一交接過程中其交接流程應明確記錄，交付人員與接收人員應填寫證據監管鏈表，詳載交件人、收件人、日期時間及目的等資訊，以示負責。

（六）數位證據識別、蒐集、擷取、封緘及運送作業流程

請參照數位證據保全標準作業流程圖辦理。

七、資安事件及數位證據編號說明

（一）資安事件編號格式：西元○年○月○日-流水編號（2 碼）。

（二）數位證據編號格式：資安事件編號-流水編號（2 碼）。