海洋委員會海巡署及所屬機關構個人資料安全維護事項作業程序

一、依據

依據個人資料保護法(以下簡稱個資法)第 4 條、第 17 條、第 18 條、個資法施行細則第 8 條、第 12 條第 2 項第 2 款、第 3 款、第 6 款、第 8 款、第 10 款規定辦理，就海洋委員會海巡署(以下簡稱本署)及所屬機關、機構(以下合稱機關)所保有之個人資料檔案，進行個人資料盤點、風險評估、風險處理及安全管理、使用紀錄、軌跡資料及證據保存及委外監督等安全維護事項作業，達成個人資料保護與管理之目標。

二、作業程序

（一）個人資料盤點

為依個資法第 18 條、個資法施行細則第 12 條第 2 項第 2 款規定，界定個人資料範圍，每年應規劃並執行個人資料盤點作業。其作業項目包括：

1. 辨識個人資料檔案：包括清查並辨識該單位於各作業流程中所使用之表單、紀錄後，由各承辦人歸納整理為個人資料檔案，並確認個人資料檔案名稱、其蒐集、處理、利用之法源、特定目的、個人資料類別、有無特定目的外利用等資訊。
2. 盤點個人資料檔案：由各單位個資專人將各承辦人個人資料檔案檢視之結果彙整後，統一製作各單位「保有個人資料盤點清冊」，並完成「保有個人資料盤點情形說明」、「個資適當安全維護措施辦理情形彙整表」(如附件 1 至附件 3)。相關清冊及資料並應妥善保管且確認其正確性。
3. 公開個人資料檔案資訊：依個資法第 17 條，保有個人資料之各機關、單位應將下列事項公開於網站，或以其他方式供公眾查詢。
   (1) 個人資料檔案名稱。
   (2) 保有機關名稱及聯絡方式。
   (3) 個人資料檔案保有之依據及特定目的。

（4） 個人資料之類別。

（二）個人資料風險評估

為依個資法第 18 條、個資法施行細則第 12 條第 2 項第 3 款規定，評估個人資料檔案之風險，每年應依前款個人資料盤點作業結果，規劃並執行個人資料風險評估作業。其項目包括：

1.個人資料風險類型識別：就盤點保有之個人資料檔案，分別依其作業情境，包含處理利用、內部傳送、保管、外部傳送、刪除銷毀、委外作業及其他等，就個別作業內容檢視及辨識其具體之風險類型，並應包括個人資料被竊取、竄改、毀損、滅失、洩漏、違反相關法令等風險。(風險類型識別得參考附件 4「風險類型暨風險對策參考表」)

2.建立風險類型及處理對策清冊：應將個人資料風險類型識別之結果及依第(三)款個人資料風險處理及安全管理作業所擬定之具體風險處理及安全管理對策，製作並完成各單位「風險類型及處理對策清冊」(如附件 5)，清冊及資料並應妥善保管且確認其正確性。

（三）個人資料風險處理及安全管理

為依個資法第 18 條、個資法施行細則第 12 條第 2 項第 6 款、第 8 款規定，規範個人資料、人員、系統設備安全管理作業，有效處理個人資料被竊取、竄改、毀損、滅失等風險，應依個人資料風險評估結果識別之風險類型，擬定具體風險處理及安全管理對策。其項目包括資料、人員、系統設備風險之處理：

1.資料風險

(1) 針對資料存取、系統存取、網路存取等設定控制機制 (例如使用憑證卡、密碼登入系統電腦，定時更新及不共用憑證密碼、設置憑證卡拔除自動系統登出及定時切換電腦螢幕保護程式、人員離開桌面淨空政策) 。

(2) 設定資料存取控制時，應考量業務性質及作業之必要，根據資料處理之方式設計之。其處理方式包含(但不限於)處理利

用、內部傳送、保管、外部傳送、刪除銷毀、委外作業及其他 (例如紙本文件專櫃上鎖存放、電子檔案加密、避免使用私人電腦、手機、社群軟體傳送含有個人資料之公務資料、使用碎紙機、文件水銷等方式確保廢棄文件不會被還原、律定傳送個人資料之類型、方式、保護及監控方式)。

(3) 律定管理者及使用者等人員職務與權限設定變更程序(例如人員異動、變更、離職、調動等因素，應立即進行權限變更、律定專責管理人員及其異動程序，禁止私自調整變動權限)。

(4) 其他資料安全管理事項，應參照本署資通安全管理規範辦理。

2.人員風險

(1) 確實掌握蒐集、處理及利用個人資料檔案之相關業務流程人員及其權責 (例如適當的職務權責區分、使用者工作所需最小權限原則、職務分工代理) 。

(2) 辦理個人資料業務時，應進行適當的安全性評估及後續落實相關人員風險評估 (例如進行適當的安全查核或資格審查、風險人員考核，避免由相關風險人員辦理) 。

(3) 明確說明機關對於個人資料保護之要求，善盡保護個人資料之義務（例如相關人員簽訂保密協定、教育訓練）。

(4) 對於違反機關個人資料保護管理規定人員應予懲處。

(5) 其他人員安全管理事項，應參照本署資通安全管理相關規範辦理。

3.系統設備風險

(1) 個人資料檔案處理之相關設備及周邊環境應有相關控管保護機制，以確保檔案之安全性，不易遭外洩及竊取之可能（例如實施實體隔離、門禁管制、安裝監視系統、系統設備應置於遠離外部人員接觸之環境、設置不透光玻璃或辦公隔板等阻隔設施）。

(2) 個人資料檔案處理，應有適當之監控措施，確保使用之軟/硬體設備為安全之控管版本，並應用防護及監控軟體進行個人資料保護及記錄 (例如防毒機制定期更新、弱點掃描、偵

測或防止惡意程式之防火牆設置、電子郵件系統防護、資訊設備和系統的紀錄檔（Log 檔）留存及防止竄改) 。

(3) 檔案資訊環境與設備之安全控管之其他規定，應參照本署資通安全管理相關規範辦理。

4.本署各單位及所屬機關就前述事項，得評估其組織業務、人員、預算等，以及個人資料之數量、敏感度等個人資料風險程度，辦理其風險處理及安全管理作業，並就高風險之個人資料檔案(例如特種個資、個資數量龐大的系統或資料庫等)優先進行處理。

（四）使用紀錄、軌跡資料及證據保存

為依個資法第 18 條、個資法施行細則第 12 條第 2 項第 10 款規定，管理與維護有關設備或紙本、電子個人資料檔案存取控制所產生之相關使用紀錄、軌跡資料、證據等。其作業項目包括：

1.使用紀錄、軌跡資料、證據範圍：包括個人資料檔案之使用紀錄或軌跡資料及其他必要之證據保存資料。其中軌跡資料指個人資料在蒐集、處理、利用過程中所產生非屬於原蒐集個人資料本體之衍生資訊（Log 檔），包括（但不限於）資料存取人之代號、存取時間、使用設備代號、網路位址（IP）、經過之網路路徑…等，可用於比對、查證資料存取之適當性。

2.使用紀錄、軌跡資料、證據之管理：

(1) 應指定個資專人管理各種使用紀錄、軌跡資料、證據。

(2) 各項使用紀錄、軌跡資料、證據之保存，依檔案法、相關法令及本署資通安全管理相關規範之規定為之。

3.使用紀錄、軌跡資料、證據之銷毀或刪除：

(1) 應定期將超過保管期限之使用紀錄、軌跡資料、證據等銷毀或刪除。

(2) 各項使用紀錄、軌跡資料、證據之銷毀或刪除，依檔案法、相關法令及本署資通安全管理相關規範之規定為之。

（五）委外監督

為依個資法第 4 條、個資法施行細則第 8 條規定，委託他人蒐集、

處理或利用個人資料時，委託機關應對受託者為適當之監督，以明責任歸屬，並確保委託處理個人資料之安全管理。各作業階段之原則及項目包括：

1.委託對象選擇階段：

(1) 研擬委託業務時應考量有無個人資料蒐集之需求並確認蒐集、處理或利用之特定目的以及是否具有個資法第 6 條、第 15 條之特定情形及符合個資法第 16 條之規定。

(2) 選擇委託對象時，應將廠商辦理個資法施行細則第 12 條第 2 項各款有關個人資料安全維護措施之情形列為評選項目。

(3) 應於委託契約載明個資法施行細則第 8 條所列監督事項及監督方式。(契約條款參考範本如附件 6)

2.業務履行階段：

(1) 應定期確認受託者執行之狀況，並將確認結果記錄之；必要時，得親自或委託專業人員進行實地訪查後，以書面敘明理由，請其限期改善；或請委外廠商依照執行現況自我檢核並提供作業說明及佐證資料，以利存查及監督委託業務執行現況。

（2） 受託者未依期限改善時，得依情節輕重，以書面通知終止或解除契約之部分或全部、要求減少部分或全部價金或按契約總價之一定比例計收違約金，並得請求損害賠償。

3.終止或解除階段：委託關係終止或解除時，應要求受託者依約定方式確實刪除、銷毀或返還因執行受託業務所保有之個人資料，並提供刪除、銷毀或返還個人資料之時間、方式、地點等紀錄；必要時，得進行實地查訪。