2017 年臺中市政府公務（含機密及敏感）資料防洩密指引

- 類型編號：20170101
- 案例標題：勞動部發現「台灣就業通」網站被駭個資外洩
- 案例闡明：勞動部勞動力發展署於 2016 年 7 月間，監控該署設置的「台灣就業通」網站時，觀測到有許多會員「同時」更改預設密碼，進一步發現會員竟都來自相同的 IP 位址，察覺有異，即刻封鎖該 IP 位址，並一併封鎖被竄改密碼成功的會員帳號，及向檢調報案，經檢調偵查發現某資產管理公司涉嫌以大量人頭帳號登入勞動力發展署「台灣就業通」網站竊取民眾個資，初估疑遭竊個資筆數逾 3 萬筆。
- 對應規範：

一、 個資法第 12 條(個人資料遭違法侵害之通知)
二、 個資法第 18 條(公務機關個人資料檔案之安全維護)
三、 個資法第 28 條(公務機關違法之損害賠償)

- 叮嚀事項：

一、 機關應避免以身分證字號作為服務系統預設帳號或密碼，預設密碼應設定為隨機亂數，提高網站過濾機制安全性。
二、 存放個人資料或敏感公務資訊之資訊系統應規範具複雜性的密碼設置原則，並制定密碼變更頻率。
三、 定期或不定期監控網站 IP 流量，即時緊急應變，防制異常登入網站情事。
四、 建立網站資料安全稽核機制。
五、 保存網站資料使用紀錄、軌跡資料及證據保存。
六、 個人資料安全維護範圍，風險評估及管理機制。
七、 建立網站資安事件之通報、預防及應變機制。
八、 網站安全管理認知宣導及教育訓練。
九、 定期或不定期系統資安演練，強化系統資安管理。
十、

- 類型編號：20170102
- 案例標題：外交部領事事務局「旅外國人動態登錄網頁」遭駭，外洩國人個資逾 1 萬 5 千筆
- 案例闡明：外交部領事事務局於 2002 年起設置「旅外國人動態登錄網頁」，提供民眾出國前登錄國人或旅行團資料及旅外停留資料，透過後端電子郵件系統，轉發民眾登錄資料至外館特定電子郵件帳號，讓駐外館處瞭解國人或旅行團動態，必要時提供國人協助，2017 年 1 月底領務局執行內部不定期資安檢測時，從 SOC 系統的 Log 中發現，自去年 10 月時，後端郵件系統突然出現大量不屬於外交部網域的 IP，因外館聯繫信箱利用特定規則產生密碼，且系統沒有重複登入嘗試的警告機制，經駭客破解密碼規則侵入，初估 3 個月內曾上「出國登錄」網站登錄的民眾個資約 1 萬 5 千筆恐遭竊取。
- 對應規範：

一、個資法第 12 條(個人資料遭違法侵害之通知)
二、個資法第 18 條(公務機關個人資料檔案之安全維護)
三、個資法第 28 條(公務機關違法之損害賠償)

- 叮嚀事項：

一、 因公務需求傳遞機敏資料或民眾個人資料，應考量資訊傳遞管道安全強度。
二、 資訊系統帳號密碼應具複雜性，避免使用具規則性或特定字母，及帳密登入監管(如：登入錯誤次數限制、異國 IP 登入警示)。
三、 定期檢視資訊系統服務狀態，及相關防禦設備紀錄，俾能儘早發現異常存取與連線行為，降低受害影響範圍。
四、 建立資安警告通報機制，掌握第一時間通報，即時危機處理。
五、 主動依個人資料保護法規定通知個人資料遭外洩之當事人，避免民眾因個資外洩受害。

- 類型編號：20170103
- 案例標題：政府機關網站遭駭，刪除民眾申請資料案
- 案例闡明：94 年 6 月刑事局偵九隊接獲某政府機關報案其電腦主機系統遭駭客入侵竄改民眾申請進入管制區資料，該系統網頁核准名冊上約 3、4 百名民眾資料遭篡改，造成機關業務運作失真，由於該機關管制地區屬軍事機敏地區，影響甚鉅，故獲關切，案經刑事局查獲涉案駭客，發現駭客是利用網路系統軟體漏洞方式，多次成功偽冒網站管理權限身分作未經授權的管理動作，侵入政府機關網站刪除部分資料，並未經政府機關同意偽冒官署名義核發電子郵件通告函取消部分經核准的民眾入境核可。
- 對應規範：

一、 刑法第 318 條之 1、之 2(洩密處罰、加重其刑)

二、 刑法第 361 條(對公務機關犯妨害電腦使用罪加重處罰)

三、 刑法第 211 條(偽造變造公文書罪)

四、 個資法第 12 條(個人資料遭違法侵害之通知)

- 叮嚀事項：

一、 定期執行系統登入管理使用權限檢視，俾即早發現未經授權管理行為。

二、 網路系統上民眾輸入資料僅限於申請項目公務處理目的使用及存取。

三、 網路系統潛存軟體漏洞，定期檢視申請民眾基本資料、使用權限帳號密碼等資料存取的安全性、完整性。

四、建立輸出輸入民眾申請資料內部監督稽核機制。

五、民眾申請經審核准駁與輸出的資料，建立相互勾稽比對制度，俾益事後檢核。

六、遠端傳輸申請審核資料採取監控紀錄(含接收者、傳送者、傳送時間、傳送資料內容、遠端傳輸 IP)的安全檢核措施。

- 類型編號：20170104
- 案例標題：某機關單一櫃檯便民服務網路系統線上申辦案件列印資料遭非申辦人本人取得案
- 案例闡明：民眾甲運用政府機關便民服務網路系統申辦業務，其線上申辦資料及查詢進度資料卻遭不明人士列印輸出，前揭資料被與申請民眾有爭訟案件的對造當事人取得，作為對其訴訟的卷證，有礙申請民眾個人隱私權益，申請人就其線上申辦案件資料遭外洩情形，向該機關請求損害賠償及追究相關疏失責任。
- 對應規範：

一、 個資法第 15 條(公務機關蒐集或處理個人資料之要件)

二、 個資法第 18 條(公務機關個人資料檔案之安全維護)

三、 個資法第 12 條(個人資料遭違法侵害之通知)

- 叮嚀事項：

一、建立輸出輸入民眾申請資料內部監督稽核制度，訂定可攜式媒體管理程序。

二、線上申辦系統傳輸資料應限縮僅顯示申請人個人資料。

三、便民服務系統資訊(含申辦進度資料、報表等)傳送予遠端申辦人時，採取安全保護措施(資料加密、監控紀錄)。

四、便民服務系統委外建置或管理者，與委外廠商簽訂資訊安全協定。

五、遠端使用者(例如申辦服務民眾)存取便民服務系統資料，宜有相關識別機制、適當監控措施，及定期或不定期稽核。

六、建置線上申辦系統備份資料相關防範洩密措施(定期備份、報廢程序、異地存放及限制使用等)。

七、宣導資安觀念，避免使用無線鍵盤、滑鼠等易遭駭工具。

類型編號：20170105

案例標題：辦理民眾臨櫃申辦業務，任意列印資料交付非被查詢者本人。

案例闡明：某政府機關服務人員疑因民眾詢問家中長輩申領相關社會福利補助事宜，該機關服務人員協助民眾而登入中央社政系統查詢民眾的長輩已領福利事項，並列印被查詢人戶籍資料，民眾向查詢者索取即帶走前揭被查詢人資料。

對應規範：

一、刑法第 318 條之 1、之 2(洩密處罰、加重其刑)

二、刑法第 361 條(對公務機關犯妨害電腦使用罪加重處罰)

三、個人資料保護法第 28 條(公務機關違法之損害賠償)

四、個人資料保護法第 15 條(公務機關蒐集或處理個人資料之要件)

叮嚀事項：

一、民眾臨櫃申辦業務，有涉及網站系統資料或個資者，應先確認申請人身分資格及事由是否合法，勿任意輕率將涉及個資或機敏業務資料隨意交付非被查詢者本人。

二、勿將透過機關網站或系統查詢所得資料或個資，隨意交付未提示證明經被查詢者本人授權委託之人，勿使用於非公務用途。

三、由中央或地方政府機關的資訊系統查得列印的資料，應隨卷歸檔或立即銷毀，避免不慎外洩。

四、機關業管單位同仁調閱各項申辦業務系統資料庫保存資料時，應記錄查詢事項(調閱事項)、調閱用途及日期(時間)，俾益事後稽核控管。

五、對於辦理民眾申辦業務運用機關網站系統查詢資料或線上申辦資料時，建立相關標準作業程序規範，記錄查詢(或使用系統)時間、人員及用途等要項，避免機關網站系統留存之機敏資料或個資不慎外洩。

- 類型編號：20170106
- 案例標題：房仲搜尋軟體業者違法破解公務機關網路系統圖形驗證碼，近 2 億個資外洩
- 案例闡明：某集團以來路不明的個資資料庫為基礎，製成「客戶開發搜尋系統軟體 V5.0 專業版」販售給房仲業者，該集團以遠端控制技術，在購買前揭軟體的業者電腦安裝內掛「圖形驗證碼破解函式」程式，方便業者任意登入公務機關伺服器，包括總統在內的 1 億 7 千筆個資全都露。經查該集團至少售出 300 套搜尋軟體，該軟體每套售價 15 至 20 萬元不等，不法所得約 6000 萬元。
- 對應規範：

一、 刑法第 358 條(入侵電腦罪)

二、 刑法第 361 條(對公務機關犯妨害電腦使用罪加重處罰)

三、 刑法第 362 條(製作程式供犯罪之用)

四、 個人資料保護法第 22 條(行政監督之權責及保密義務)

五、 個人資料保護法第 18 條(公務機關個人資料檔案之安全維護)

六、 個人資料保護法第 12 條(個人資料遭違法侵害之通知)

- 叮嚀事項：

一、 機關網站系統公開民眾個人資料，應於公開前研擬資料揭露範圍，宜採行僅揭露去識別化個人資料措施，避免完整揭露民眾姓名、住址資料等個資。

二、 主管機關建立定期查核民間企業使用機關網站系統揭露民眾個人資料的機制，期能即時採取防弊措施。

三、 限制民間業者自下載機關網站系統揭露的民眾個資筆數，禁止批次下載申請功能，以避免個資大量外洩。

四、 機關網站建置慎選委外廠商，妥善研擬簽定委外契約條款，並定期專人監控委外廠商執行情形。

五、 建立機關 e 化資料庫安全管理機制，落實內部稽核。