臺灣學術網路個資外洩事件之預防與應變指南

臺灣學術網路危機處理中心團隊(TACERT)製

2020 年 04 月 第二版

一、 前言

為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，制定個人資料保護法（以下稱個資法）。個資法之保護客體，不限於經電腦處理之個人資料，且以任何形式存在之個人資料皆有該法之適用。個資法之保護適用範圍涵蓋公務機關與非公務機關均有適用，舉凡涉及個人資料蒐集、處理、利用之個人、法人或團體皆為該法之適用，且各行各業皆應適用該法。個人資料蒐集、處理與利用之行為規範，諸如：告知義務之履行，並提高損害賠償之額度且導入團體訴訟之機制。此外，因應實務運作之需求，將病歷納入特種個人資料之範圍，當事人書面同意為特種個人資料之蒐集、處理與利用依據。

近期因學術網路發生個人資料遭不當揭露或利用之情況頻傳，應維護個人資料安全，避免個資外洩之威脅。因此，強化臺灣學術網路資通安全管理機制的個人資料保護有效性與避免個資外洩資安事件發生日漸重要，在本文中 TACERT 將以個資事件發生的三個階段「事前預防、事發應變和事終檢討」進行說明，作為學校在處理個資外洩資安事件的參考指南。

二、 個人資料定義與個資外洩事件種類

個人資料的定義(以下簡稱個資)，是指任何關於可識別個人或足資識別該個人之資料，包括有自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動，以及其他得以直接或間接方式識別該個人之資料。另外，特種個人資料包括有關病歷、醫療、基因、性生活、健康檢查及犯罪前科等內容。

個資外洩事件可依其洩漏途徑的不同，區分為「駭客入侵竊取」、「設備送修、遺失或被竊」、「過期資料未銷毀」及「網站上的數據洩漏」等四種。從臺灣學術網路個資外洩之案例，發現來自網站上的數據洩漏事件較常見，

因此，本文以提供此類個資外洩事件的預防與應變措施為主要目標。

三、 個資外洩事件之事前預防

從資安管理之事前預防方面，建議以個資法施行細則第 12 條所規定之 11 項安全維護措施，作為事前的預防因應。詳細說明請參考附錄 A 之安全維護措施。

1. 配置管理之人員及相當資源。

2. 界定個人資料之範圍。

3. 個人資料之風險評估及管理機制。

4. 事故之預防、通報及應變機制。

5. 個人資料蒐集、處理及利用之內部管理程序。

6. 資料安全管理及人員管理。

7. 認知宣導及教育訓練。

8. 設備安全管理。

9. 資料安全稽核機制。

10. 使用紀錄、軌跡資料及證據保存。

11. 個人資料安全維護之整體持續改善。

若從技術層面來探討預防措施，可以以學術網路中造成個資外洩事件的常見原因來分類，並且分述其原因與防範建議如下。

1. 網頁應用程式設計未做安全檢測

程式設計師在撰寫網頁程式時未做資安考量來修補程式漏洞，容易造成像 SQL Injection 之類的漏洞攻擊，造成非法使用者存取到資料庫內容，進而外洩個資資訊。針對此外洩原因建議防範措施如下:

(1). 建議執行網頁程式源碼檢測。

(2). 定期網站弱點檢測。可向「EVS 教育單位弱點檢測平臺」申請弱點掃描，發現並修正網站潛在威脅。

(3). 建議根據 OWASP 網頁安全指引，檢視網站安全，並修復可能之風險。

(4). 為增加網站安全性，建議安裝網站應用程式防火牆(Web Application Firewall，簡稱 WAF)，強化網站安全性。

2. 未遮蔽之個資檔案誤置於網站中，或網站內早期個資檔案使用期限結束未銷毀

常見學校在公告時誤將未遮蔽個資的檔案（多為 xlsx、pdf 或 doc 等文件類型檔案）以公告之附件下載連結或過期公告檔案未刪除等方式置於網站上，導致該檔案被下載。針對此外洩原因建議防範措施如下:

(1). 定期檢視存放於網站上之公告附件檔案內資訊是否合宜。

(2). 使用搜尋引擎的查詢語法，檢查是否有個資可能被不當的存取。例如，filetype:xlsx site:XX.edu.tw，查詢 XX 學校網域中，檔案類型為 xlsx 的檔案。

3. 對於上傳檔案至網站的功能未進行權限控管與限制上傳檔案類型

網站的檔案上傳功能若未檢測其上傳檔案之合法性，或未做權限控管，可能導致有心人士上傳惡意程式至網站，進而竊取個資資訊或進行網路攻擊。針對此可能造成個資外洩的原因提供以下兩點事先預防措施。

(1). 盤點網站資料內容與檢視系統功能，並且確認網站是否設定適當的權限控管。

(2). 針對網站應用程式增加檢測上傳檔案之合法性。

4. 主機系統帳戶密碼與網站管理者帳戶密碼使用弱密碼

若網站主機的作業系統登入帳戶或網站管理者帳戶使用弱密碼，將導致攻擊者暴力破解密碼後登入到網站後端系統，進而存取到與個資有關的資料。

(1). 盤點網站與系統內各資料夾的存取權限，並確認設定適當的權限與存取控管。

(2). 強化帳戶之密碼安全性，並且定期更換密碼。

四、 個資外洩事件之事發應變

當學校接獲資安通報單或外部情資(如 HITCON Zero Day)通知有個資外洩事件時，有下列處理方式提供學校參考。

1. 確認事件的真實性與了解事件原因

學校在第一時間被告知時，需確認事件的真實性，並了解外洩的網址、外洩的原因、外洩資料筆數與外洩的個資欄位等內容，進而評估出該事件的影響範圍。若該事件是由外部情資告知而知悉，需至教育機構資安通報平台(https://info.cert.tanet.edu.tw/)進行自行通報作業。另依據資通安全管理法規範，學校在知道該事件為資安事件時，需於知悉後一個小時內完成資安事件的通報作業。

2. 確認是否需要資安專業人員的協助

有鑑於個資外洩事件發生的原因除了人為失誤造成外，多半是因為網站資訊洩漏導致個資被不恰當存取。因此，探討網站資訊如何被洩漏與了解個資外洩檔案被存取狀況變得極為重要。根據個資外洩事件的嚴重層級，學校可評估事件狀況來請決定是否需要資安專業人員的協助。若有資安專業人員協助，學校可針對網站主機進行鑑識作業或網站日誌分析，以便深入了解資訊洩漏的原因與外洩檔案被存取的情形。

3. 將外洩個資檔案從網站上移除

當學校確認為個資外洩事件後，應立即將外洩檔案從外洩網址之處移除，以避免其個資資料持續外洩及遭他人利用。

4. 保存個資外洩事件的證據

當個資外洩事件發生後，學校除了盡快將外洩檔案從網站上移除外，對於與個資外洩事件有關的資料，如:個資外洩事件的原因、外洩資

料筆數、外洩資料欄位、網站日誌、網站主機的系統日誌、整個事件處理過程中的證據、、、等等皆需妥善保存，以便作為日後若有調查需求時之參考證據。

5. Google 搜尋引擎申請移除外洩檔案之暫存頁面

因 Google 會定期針對各網站內容進行爬文，為避免他人經由 Google 庫存頁查詢方式，取得個資外洩檔案之相關資訊。學校可根據以下連結的說明，申請移除相關資訊。申請 Google 移除資訊網址:

https://support.google.com/websearch/troubleshooter/3111061?hl=zh-Hant&rd=1。

6. 個資外洩公告

依個人資料保護法第 12 條及施行細則第 22 條規定(如下列兩點內容)，學校在處理完成前述各步驟後，需以適當方式通知個資外洩當事者。其通知內容應包括個人資料被侵害之事實，以及學校已採取之因應措施。若外洩資料筆數過大，無法個別通知當事人。在考量技術可行性與保護當事人隱私的情況下，可透過網際網路、新聞媒體或其他適當公開方式通知。

(1). 個人資料保護法第 12 條

公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。

(2). 個人資料保護法施行細則第 22 條

本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施。

五、 事終檢討與未來防範

在個資外洩事件發生後，建議學校以制度面、管理面及技術面等方面，檢討單位內如何改善並實施安全控管。經觀察學術網路內的個資外洩事件，發現經由網站將個資資料外洩的比例很高。因此，針對網站安全與個資的防護，整理下列改善措施提供學校參考。

1. 制度面

(1). 加強個人資料保護法與相關規定的宣導

個人資料保護法從 103 年起實施至今已將近 6 年，但每當有個資外洩事件發生時，有部分原因是因校內業務人員不慎造成。因此，建議學校多多加強個資法的宣導。

(2). 建議可於校內成立個資小組，來定期審核校園內個資防護措施的實施情形。

2. 管理面

(1). 檢視現有網站內檔案內容是否存在個資資訊

因 103 年以前個資法尚未實施，學校業務人員無個資概念，放置網站的檔案容易有未遮蔽個資的情形。故在檢視時需特別留意是否由 103 年以前的檔案存放於網站內。

(2). 檢視網站內是否有已刪除之公告，但附件檔案仍未刪除之情形，建議查看此類型檔案內是否存在個資資訊。

(3). 加強網站管理者帳戶與網站主機帳戶之密碼強度。

(4). 檢視網站資料存取的權限與管控設定。

(5). 查看網站檔案上傳功能之權限設定是否適當與確認上傳的檔案類型是否正確。

(6). 建議網站管理者不同時使用同一組帳號與密碼管理多台網站主機。

(7). 對於學生上傳至網站之個人學習報告或個人證照，建議確認檔案內

是否存在個資內容，常發現學生證照上印有學生個人身分證字號。

(8). 定期備份網站主機資料。

(9). 對於學校委外建置之網站系統，建議於採購時要求在驗收時提供網站之源碼檢測與弱點掃描作業的報告。

3. 技術面

(1). 建議對現有運作中的網站系統進行源碼檢測、弱點掃描與滲透測試並針對檢測結果進行程式修補作業。

(2). 定期更新網站主機的作業系統與防毒軟體。

(3). 定期檢視網站程式碼之安全性，並且修補資安漏洞。

(4). 建議勿使用身分證字號作為網站登入帳號。

(5). 定期對網站主機進行掃毒作業。

(6). 檢視網站主機對外所開啟的 port 是否有必要使用之情形，建議關閉駭客常會攻擊的 Port，如 445port 與 3389port。

(7). 在網站主機的維護方面，如需使用 RDP 方式進行連線，建議限制連線主機的來源 IP。

六、 參考資料

[1]. 個人資料保護法
https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

[2]. 個人資料保護法施行細則
https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050022

[3]. OWASP 組織所發佈的網頁安全指引 (OWASP top 10)
https://owasp.org/www-project-top-ten/

[4]. 申請 google 庫存頁的移除
https://support.google.com/websearch/troubleshooter/3111061?hl=zh-Hant&rd=1

[5]. 申請「EVS 教育單位弱點檢測平臺 」
https://evs.twisc.ncku.edu.tw/

附件 A、 11 項安全維護措施

根據個資法施行細則第 12 條所規定之 11 項安全維護措施詳列如下內容，而個資法所提到「適當安全維護措施、安全維護事項與適當之安全措施」，是指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，所採取技術上及組織上之措施。

一、 配置管理之人員及相當資源

因應組織架構，個資管理負責人其作用在傳達管理組織所吩咐的工作，以落實個資管理安全措施的要求。

二、 界定個人資料之範圍

1. 用個資盤點找出學校內部所有個人資料。
2. 要從個資生命周期來盤點個資。
3. 找出任何存放個資的載具，包括紙本或電子形式的個資。
4. 可藉助盤點工具加快清查速度，但須了解盤點工具的侷限。

三、 個人資料之風險評估及管理機制

1. 降低-設計控管程序降低風險發生之可能性。
2. 迴避-放棄可能會產生風險的業務流程。
3. 接受-訂定該風險之衝擊屬於可接受之範圍，不進行任何處理。
4. 轉嫁-將風險結果請求他人協助分擔，例如保險或賠償基金。

四、 事故之預防、通報及應變機制

1. 依不同風險等級來制定通報應變程序和通報對象。
2. 個資事故依法必須通知個資當事人。
3. 從事故中記取教訓找出預防措施。
4. 積極處理事故，若處理得宜，可補救形象。

五、 個人資料蒐集、處理及利用之內部管理程序

1. 應有特定目的，並符合下列情形（個資法第 19 條）

   (1). 法律明文規定。

   (2). 當事人自行公開或其他已合法公開之個人資料。

(3). 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別。例如，研究機構為了統計我國因癌症死亡之機率，而蒐集相關醫療資訊。如果可連結特定當事人之資料，如姓名、住址、病歷編號等等，均未提供給研究機構，由於無法識別特定當事人，即符合此款規定之情形。

(4). 經當事人書面同意。書面同意，依照施行細則第 14 條，亦可以電子文件為之。

(5). 與公共利益有關。

(6). 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。個資法第 19 條修法說明指出，由於資訊科技及網際網路之發達，個人資料之蒐集、處理或利用甚為普遍，尤其在網際網路上張貼之個人資料其來源是否合法，經常無法求證或需費過鉅，為避免蒐集者動輒觸法或求證之行為曠日費時，明定個人資料取自於一般可得之來源者，亦得蒐集或處理。

2. 應明確告知當事人下列事項（個資法第 8 條）

(1). 公務機關或非公務機關名稱。

(2). 蒐集之目的。

(3). 個人資料之類別。

(4). 個人資料利用之期間、地區、對象及使用方式。

(5). 當事人依第 3 條規定得行使之權利及方式。

(6). 當事人得自由選擇提供個人資料時，不提供將對其權益之影響。

3. 下列情形，始得為目的外利用（個資法第 20 條）

(1). 法律明文規定。

(2). 為增進公共利益。

(3). 為免除當事人之生命、身體、自由或財產上之危險。

(4). 為防止他人權益之重大危害。

(5). 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

(6). 經當事人書面同意。

六、 資料安全管理及人員管理

1. 資料要分級管理，可依資料敏感程度、風險高低來分級並訂定不同管理方法。
2. 個資使用或傳輸時若沒有必要完整顯示時，就要部分遮罩或去識別化處理。
3. 建立紙本文件與電子檔案的存取控管流程。
4. 內含個資的資料傳輸過程要加密以避免外洩。
5. 要依職務分級管理個資存取權限。

七、 認知宣導及教育訓練

此為個資法針對個人資料安全維護事項之規定，應指派教育訓練負責人實施教育訓練，同時，也應留下教育訓練之記錄，以供日後參考，並且作為已符合個資法規範要求之證明。

八、 設備安全管理

1. 凡是可儲存個資的設備，不論是固定設備或行動設備都要納入制度管理。
2. 設備管理政策要充分告知。
3. 存放大量個資的資料庫及機房要嚴加控管。

九、 資料安全稽核機制

個資安全事故之改善、預防措施及事故發生單位應列為內部稽核作業之重要查核範圍，並辦理追蹤考核。

十、 使用紀錄、軌跡資料及證據保存

1. 要從日後訴訟舉證角度來保存各種軌跡證據使用記錄。
2. 管理文件控管來保存紙本文件。
3. Log 檔只需保存必要欄位來減量。
4. Log 檔管理人員不能擁有 Log 修改與刪除權限。

5. 個資使用記錄和軌跡記錄至少要保存 5 年。

十一、 個人資料安全維護之整體持續改善

1. 要定期持續檢討，並非發生事故才需要改善。
2. 三種常見需持續改善的情況：內外部稽核報告的矯正要求、法規修改或是驗證單位要求、單位營運事項更動以及其他重大變故。
3. 主管定期召開審查會議，審視個資保護制度落實程度。
4. 持續改善制度文件、會議記錄與實施記錄都要保留。