內政部　函

地　　址：100218 臺北市中正區徐州路 5 號
傳　　真：(02)2356-6226
承 辦 人：張家榮
連絡電話：(02)2356-5426
電子信箱：moi1857@moi.gov.tw

受文者：中華民國全國商業總會
發文日期：中華民國 115 年 3 月 20 日
發文字號：台內團字第 11502817382 號
速別：普通件
密等及解密條件或保密期限：
附件：如文(共 2 個附件：301000000A115028173803-1.pdf、301000000A115028173803-2.pdf)（301000000A115028173803-1.pdf、301000000A115028173803-2.pdf，共二個電子檔案）

主旨：檢送「個人資料保護與人民團體／合作社」宣導資料 1 份，請惠予協助向會員宣導，請查照。

說明：

一、依據「內政部輔導非公務機關提升個人資料保護意識及反詐騙宣導計畫」辦理。

二、按個人資料保護法第 2 條，非公務機關係指公務機關以外的自然人、法人或其他團體。鑒於非公務機關所持有之個人資料外洩事件頻傳，不僅引起社會大眾高度關注，遭外洩之個資亦容易遭不法集團不當使用，為提升非公務機關之個資防護能力，本部爰訂定前開計畫，針對業管非公務機關加強輔導。

三、依本部 110 年 11 月 30 日台內團字第 1100282042 號令發布「內政部指定合作及人民團體類非公務機關個人資料檔案安全維護管理辦法」第 3 條規定，該辦法所稱非公務機關包括各級人民團體等，為提升人民團體之個資保護意識，特製作旨揭宣導資料，分為「個人資料保護法」及「內政

個人資料保護與人民團體／合作社

內政部合作及人民團體司

115年3月

什麼是個人資料？

基本識別資訊

包含姓名、出生年月日、身分證字號、護照號碼等得以直接識別個人的基礎資料。

敏感與特徵資訊

包含指紋、特徵、病歷、醫療、基因、性生活、健康檢查及犯罪前科等高度敏感資料。

社會與生活資訊

包含婚姻、家庭、教育、職業、聯絡方式、財務情況、社會活動等生活軌跡資料。

蒐集與利用的「黃金守則」

☑ 必須做 (義務)

- 尊重當事人權益，依誠實及信用方法為之。
- 明確告知當事人：機關名稱、蒐集目的、資料類別、利用之期間/地區/對象/方式。
- 告知當事人依法得行使之權利及方式。
- 非公務機關蒐集時需符合法律明文規定或與當事人有契約關係等要件。
- 採取適當安全維護措施，防止資料外洩。

✕ 不能做 (限制)

- 不得逾越特定目的之必要範圍。
- 不得將個人資料為處理以外之不當使用。
- 原則上不得蒐集、處理或利用醫療、基因、犯罪前科等高度敏感個資（除非法律明文規定等例外）。
- 當事人表示拒絕接受行銷時，應立即停止利用其個資行銷。

違反個資法的代價與風險

不可輕忽的法律責任：

💰 民事損害賠償

若無法證明實際損害額，法院可判定每人每一事件 500 至 2 萬元賠償；單一事件最高總額可達新臺幣 2 億元！

≡ 行政罰鍰

未依規定採行安全措施等，經限期未改善，最高可按次處新臺幣 1,500 萬元罰鍰，代表人亦須受同一額度處罰。

⚖ 刑事責任

意圖營利或損害他人利益而違法蒐集/利用，或非法竄改檔案者，最高可處 5 年以下有期徒刑。

🎯 誰需要訂定「安全維護計畫」？

5,000

筆個資門檻

合規啟動關鍵

非公務機關保有會(社)員之個人資料達 5,000筆 者，應訂定個人資料檔案安全維護計畫及會(社)務終止後處理方法。

🕒法定期限：

須於完成立案或達標之日起 **6個月內** 報請主管機關備查！

資通訊系統專屬防護措施

(適用於使用資通訊系統處理達 5,000 筆以上個資者)

認證 建立使用者身分確認及保護機制，防止未授權登入。

隱碼 系統顯示個人資料時，應具備隱碼機制（例如：陳O明、A12****789）。

加密 透過網際網路傳輸個人資料時，須採取安全加密機制。

控管 嚴格實施個資檔案與資料庫的存取控制及保護監控措施。

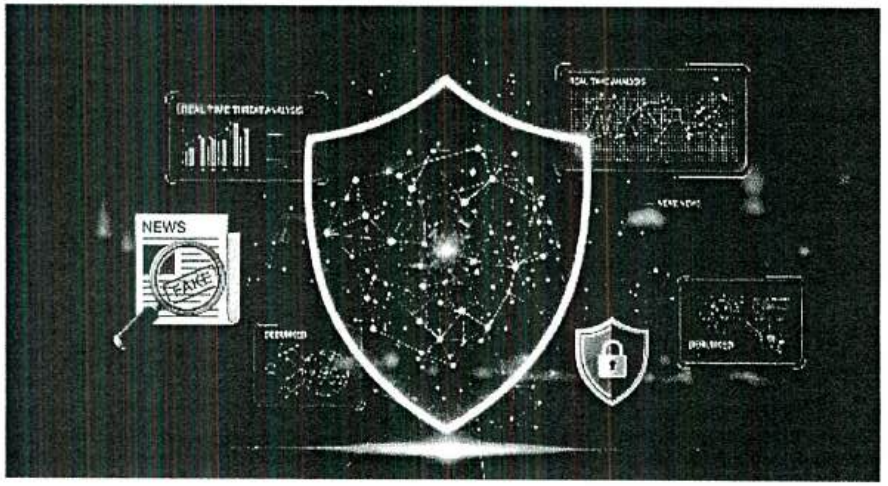
防護 建置防止外部網路入侵對策，並監控非法或異常使用行為（需定期演練）。

萬一發生事故怎麼辦？ (SOP)

⚠緊急應變流程

第一步：控制與通知 採取即時有效之應變措施控制損害，並查明事故後以適當方式通知當事人（包含事實、因應措施及諮詢專線）。

第二步：【黃金 72 小時】**通報** 遇有達 1,000筆以上之外洩事故，須於發現後 **72小時內** 以書面通報直轄市/縣市政府，並副知內政部。



有任何問題嗎?

感謝聆聽！讓我們一起建構安全可信賴的個資保護環境。

內政部指定合作及人民團體類非公務機關個人資料檔案安全維護管理辦法

第一條　本辦法依個人資料保護法（以下簡稱本法）第二十七條第三項規定訂定之。

第二條　本辦法所稱主管機關：在中央為內政部；在直轄市為直轄市政府；在縣（市）為縣（市）政府。

第三條　本辦法所稱非公務機關，包括下列各款：

一、各級人民團體、合作社及儲蓄互助社。

二、其他經中央主管機關公告指定者。

第四條　非公務機關保有會（社）員之個人資料達五千筆者，應訂定個人資料檔案安全維護計畫及會（社）務終止後個人資料處理方法（以下簡稱本計畫及處理方法），以落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

非公務機關依前項規定訂定本計畫及處理方法時，應視其組織規模、特性、保有個人資料之性質及數量等事項，參酌第五條至第二十一條規定，訂定包含下列各款事項之適當安全維護管理措施；必要時，第二款各目事項得整併之：

一、非公務機關之組織規模及特性。

二、個人資料檔案之安全管理措施：

（一）配置管理之人員及相當資源。

（二）界定蒐集、處理及利用個人資料之範圍。

（三）個人資料之風險評估及管理機制。

（四）事故之預防、通報及應變機制。

（五）個人資料蒐集、處理及利用之內部管理程序。

（六）設備安全管理、資料安全管理及人員管理措施。

（七）認知宣導及教育訓練。

（八）個人資料安全維護稽核機制。

（九）使用紀錄、軌跡資料及證據保存。

（十）個人資料安全維護之整體持續改善。

（十一）會（社）務終止後之個人資料處理方法。

後七十二小時內將通報機關、發生時間、發生種類、發生原因及摘要、損害狀況、個人資料侵害可能結果、擬採取之因應措施、擬通知當事人之時間及方式、是否於發現個人資料外洩後立即通報等事項，以書面通報其主管機關。如為直轄市、縣（市）主管機關接獲通報，並應副知中央主管機關（書面通報格式如附件）。

主管機關對於重大個人資料事故，得依本法第二十二條規定對非公務機關之應變、通報及預防機制進行實地檢查，並視檢查結果為後續處置。中央主管機關認有必要時，得督導直轄市、縣（市）主管機關對於非公務機關之相關機制改善情形。

第九條　非公務機關所屬人員為執行會（社）務而蒐集、處理一般個人資料時，應檢視是否符合本法第十九條之要件；利用時，應檢視是否符合蒐集之特定目的必要範圍；為特定目的外之利用時，應檢視是否符合本法第二十條第一項但書情形。

第十條　非公務機關蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求所屬人員確實辦理。

第十一條　中央主管機關依本法第二十一條規定，對非公務機關為限制國際傳輸個人資料之命令或處分時，非公務機關應通知所屬人員遵循辦理。

非公務機關將個人資料作國際傳輸者，應檢視是否受中央主管機關限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督：

一、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

二、當事人行使本法第三條所定權利之相關事項。

第十二條　非公務機關於個人資料當事人行使本法第三條規定之權利時，應依下列規定辦理：

一、提供聯絡窗口及聯絡方式。

二、確認為個人資料當事人本人，或經其委託者。

第十五條　非公務機關使用資通訊系統蒐集、處理或利用會（社）員個人資料達五千筆以上者，應採取下列資訊安全措施：

一、使用者身分確認及保護機制。

二、個人資料顯示之隱碼機制。

三、網際網路傳輸之安全加密機制。

四、個人資料檔案與資料庫之存取控制及保護監控措施。

五、防止外部網路入侵對策。

六、非法或異常使用行為之監控及因應機制。

前項第五款及第六款所定措施，應定期演練及檢討改善。

第十六條　非公務機關應定期或不定期對於所屬人員施以基礎個人資料保護認知宣導及教育訓練，使其明瞭相關法令之要求、所屬人員之責任範圍與各種個人資料保護事項之機制、程序及措施。

第十七條　非公務機關為確保本計畫及處理方法之落實，應依其組織規模及特性，衡酌資源之合理分配，訂定個人資料安全維護稽核機制，並指定適當人員每半年至少進行一次本計畫及處理方法執行情形之檢查。

前項檢查結果應向代表人提出報告，並留存相關紀錄，其保存期限至少五年。

非公務機關依第一項檢查結果發現本計畫及處理方法不符法令或有不符法令之虞者，應即改善。

第十八條　非公務機關執行本計畫及處理方法所定各種個人資料保護機制、程序及措施，應記錄其個人資料使用情況，留存軌跡資料或相關證據。

非公務機關依本法第十一條第三項規定刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

一、刪除、停止處理或利用之方法、時間或地點。

二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間、地點，及該對象蒐集、處理或利用之合法依據。

第八條附件

<table>
<tr><td colspan="3">個人資料事故通報及紀錄表</td></tr>
<tr><td>非公務機關名稱
＿＿＿＿＿＿
通報機關
＿＿＿＿＿＿</td><td colspan="2">通報時間：　　年　　月　　日　　時　　分
通報人：　　簽名（蓋章）
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">發生種類</td><td rowspan="2">□竊取
□竄改
□毀損
□滅失
□洩漏
□其他侵害情形</td><td>個人資料侵害之總筆數（大約）
＿＿＿＿＿＿</td></tr>
<tr><td>□一般個人資料 ＿＿＿＿筆
□特種個人資料 ＿＿＿＿筆</td></tr>
<tr><td>發生原因及摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個人資料侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個人資料外洩後七十二小時內通報</td><td colspan="2">□是　□否，理由：</td></tr>
</table>

備註：特種個人資料，指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料；一般個人資料，指特種個人資料以外之個人資料。