檔　　號:
保存年限:

全聯不動產收文 113年3月05日 第15486號

內政部國土管理署 函

地址：105404臺北市松山區八德路2段342號
聯絡人：黃一峯
聯絡電話：02-87712776
電子郵件：hyif112035@cpami.gov.tw
傳真：02-87712876

受文者：中華民國不動產開發商業同業公會全國聯合會

發文日期：中華民國113年3月5日
發文字號：國署住字第11300174091號
速別：普通件
密等及解密條件或保密期限：
附件：如說明二（1131034488_11300174091_113D2007020-01.pdf、1131034488_11300174091_113D2007021-01.pdf、1131034488_11300174091_113D2007022-01.pdf）

主旨：函轉「內政部輔導非公務機關提升個資保護意識及防護措施計畫」（下稱本計畫），請貴公會協助宣導，詳如說明，請查照。

說明：

一、依據本部113年2月5日台內法字第1130401027號函、「內政部指定營建類非公務機關個人資料檔案安全維護管理辦法」（下稱本辦法）及本計畫辦理。

二、依本計畫第4點，檢送本辦法、本計畫及「個人資料檔案安全維護計畫或業務終止後個人資料處理方法（下稱處理方法）（範本）」1份，惠請協助向貴會會員宣導訂定處理方法，並依限報請直轄市、縣（市）政府備查。

正本：中華民國不動產開發商業同業公會全國聯合會
副本：電子公文交換章 2024/03/05 11:38:06

內政部輔導非公務機關提升個資保護意識及防護措施計畫

112年5月8日台內法字第11204006722號函訂定
112年9月22日台內法字第1120401545號函修正
113年1月31日台內法字第1130401004號函修正

一、目的及依據

鑒於非公務機關所持有之個人資料（以下簡稱個資）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，依據行政院112年3月2日第3845次院會會議決定，內政部（以下簡稱本部）特訂定本計畫。

二、執行單位及機關

本部民政司、戶政司、地政司、宗教及禮制司、合作及人民團體司、警政署、移民署及國土管理署。

三、輔導對象

本計畫之輔導對象為以下辦法之規範對象：

（一）內政部指定政黨及全國性民政財團法人個人資料檔案安全維護管理辦法。

（二）內政部指定交友服務業個人資料檔案安全維護管理辦法。

（三）內政部指定地政類非公務機關個人資料檔案安全維護管理辦法。

（四）內政部指定祭祀團體個人資料檔案安全維護管理辦法。

（五）內政部指定宗教團體個人資料檔案安全維護管理辦法。

（六）內政部指定殯葬服務業個人資料檔案安全維護管理辦法。

（七）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。

（八）內政部指定警政類非公務機關個人資料檔案安全維護管理辦法。

（九）內政部指定移民業務機構個人資料檔案安全維護管理辦法。

（十）內政部指定營建類非公務機關個人資料檔案安全維護管理辦法。

四、 提升業者個資保護意識之規劃

（一）措施內容

1、對非本部直接轄管之輔導對象：執行單位及機關應提供相關宣導資料，函請直轄市、縣（市）政府、全國性及地方性相關公會協助宣導。

2、對本部直接轄管之輔導對象：執行單位及機關應辦理個資保護教育座談會或課程，亦得併例行性業務檢查辦理。

（二）推動時程：每年度至少辦理一次。

（三）預期效益：增進輔導對象之個資保護意識。

五、 輔導業者強化個資防護措施

（一）措施內容

1、對非本部直接轄管之輔導對象：執行單位及機關應督導各直轄市、縣（市）政府針對未訂定「個人資料檔案安全維護計畫及業務終止後個人資料處理方法」之輔導對象進行一般業務檢查，並適時要求輔導對象依相關規定辦理。

2、對本部直接轄管之輔導對象：執行單位及機關應督促未訂定「個人資料檔案安全維護計畫及業務終止後個人資料處理方法」之輔導對象儘快依相關規定辦理；另因取得個資保護管理或資訊安全驗證之條件複雜，經費需求亦高，爰得僅對已上市之輔導對象宣導鼓勵其通過相關認證。

（二）推動時程：每年度至少辦理一次。

（三）預期效益：提升輔導對象採取強化相關防護措施之效果。

六、 各執行單位及機關得視業務需要，針對所轄（包含直接或非直接轄管）之輔導對象，訂定提升個資保護意識及防護措施計畫。

七、 管理考核

執行單位及機關應於每月5日前，將前一月辦理情形及相關附件送交本部法制處，俾利回報個人資料保護委員會籌備處。

法規名稱：內政部指定營建類非公務機關個人資料檔案安全維護管理辦法
發布日期：民國 110 年 11 月 30 日

第 1 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 2 條

本辦法所稱主管機關，在中央爲內政部；在直轄市爲直轄市政府；在縣（市）爲縣（市）政府。

第 3 條

1 本辦法所稱非公務機關，包括下列各款：
一、營造業。
二、不動產開發業。
三、建築師事務所。
四、公寓大廈管理維護公司。
五、都市更新業務財團法人。
六、其他經中央主管機關公告指定者。
2 前項第二款不動產開發業，指以銷售爲目的，從事土地、建物等不動產投資興建之行業。

第 4 條

1 非公務機關應訂定個人資料檔案安全維護計畫及業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。
2 非公務機關依前項規定訂定本計畫及處理方法時，應視其業務規模、特性、保有個人資料之性質及數量等事項，參酌第五條至第二十三條規定，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）業務終止後之個人資料處理方法。
3 第一項之本計畫及處理方法，都市更新業務財團法人應於主管機關許可設立之日起六個月內報請其主管機關備查，其餘非公務機關應於開業或完成營業項目登記之日起六個月內，報請主事務所所在地之直轄市、縣（市）主管機關備查。
4 中央主管機關依前條第一項第六款公告指定前，已完成開業、營業項目登記或財團法人許可設立者，應於公告指定之日起六個月內，將第一項之本計畫及處理方法報請主事務

所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。

第 5 條

1 非公務機關應配置適當管理人員及相當資源，負責規劃、訂定、修正及執行本計畫及處理方法等相關事項，並定期向負責人提出報告。

2 非公務機關應訂定個人資料保護管理政策，將蒐集、處理及利用個人資料之特定目的、法律依據及其他相關保護事項，公告於營業處所或主事務所適當之處；如有網站者，並揭露於網站首頁，使其所屬人員及個人資料當事人均能知悉。

第 6 條

非公務機關應界定納入本計畫及處理方法之個人資料範圍，辦理下列事項：

一、定期清查保有之個人資料現況。

二、確認保有之個人資料所應遵循適用之個人資料保護相關法令現況。

第 7 條

非公務機關應依前條已界定之個人資料範圍及蒐集、處理、利用個人資料之流程，評估可能產生之風險，並根據風險評估之結果，依風險等級訂定適當之管控措施。

第 8 條

非公務機關爲因應保有之個人資料被竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱個人資料事故），應採取下列應變、通報及預防機制：

一、採取適當之應變措施，以控制個人資料事故對當事人之損害，並通報內部有關單位。

二、查明個人資料事故之狀況並以適當方式通知當事人有關個人資料事故事實、所爲因應措施及諮詢服務專線等內容。

三、研議預防機制，避免類似個人資料事故再次發生。

第 9 條

1 非公務機關依前條第一款通報者爲重大個人資料事故，應於發現後七十二小時內，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、是否於發現事故後立即通報等事項，以書面通報主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關；如爲直轄市、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）。

2 前項所稱重大個人資料事故，指個人資料被竊取、竄改、毀損、滅失或洩漏達一千筆以上，將危及非公務機關正常營運或大量當事人權益之情形。

3 主管機關接獲通報或主動知悉事故，得依本法第二十二條至第二十五條規定所賦予之職權，爲適當之監督管理措施。

第 10 條

非公務機關所屬人員對於個人資料蒐集、處理及利用，應注意下列事項：

一、屬本法第六條所定特種個人資料者，應檢視其特定目的及是否符合相關法令之要件；其經當事人書面同意者，應符合本法第七條第一項、第二項及第四項規定。

二、檢視一般個人資料之蒐集、處理，是否符合本法第十九條規定，具有特定目的及法定要件。其經當事人同意者，應符合本法第七條第一項、第三項及第四項規定。

三、檢視一般個人資料之利用，是否符合本法第二十條規定，於蒐集之特定目的必要範圍內爲之；特定目的外之利用，是否符合本法第二十條第一項但書規定。其經當事人同意者，應符合本法第七條第二項及第四項規定。

四、利用個人資料爲行銷，當事人表示拒絕行銷後，立即停止利用其個人資料行銷，且周知所屬人員，並至少於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。

五、於蒐集、處理或利用過程中，檢視個人資料是否正確，有不正確時，應主動更正或補充。其正確性有爭議者，應依本法第十一條第二項規定辦理。

第 11 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 12 條

1 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。

2 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 13 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。

三、認有本法第十條但書各款、第十一條第二項但書或第三項但書規定得拒絕當事人行使權利之事由時，應附理由通知當事人。

四、有收取必要成本費用者，應告知當事人收費基準。

五、遵守本法第十三條有關處理期限之規定。

第 14 條

非公務機關為維護所保有個人資料之安全，使用存有個人資料之各類設備或儲存媒體，應採取下列資料安全管理措施：

一、運用電腦或自動化機器相關設備蒐集、處理或利用個人資料時，訂定各類設備或儲存媒體之使用規範。

二、針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，採取適當之加密機制。

三、作業過程有備份個人資料之需要時，該備份資料比照原件，依本法規定予以保護之。

四、存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物，於報廢、汰換或轉作其他用途時，應採適當防範措施，以避免由該媒介物洩漏個人資料；委託他人執行者，非公務機關對受託人之監督依第二十二條規定辦理。

第 15 條

1 非公務機關使用資通訊系統蒐集、處理或利用個人資料，且其資料庫保有個人資料數量達五千筆以上者，應採取下列措施：

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。

2 前項第五款及第六款所定措施，應定期演練及檢討改善。

第 16 條

1 非公務機關對保有個人資料之環境及實體設備安全，應採取下列措施：

一、依據作業內容之不同，實施適宜之進出管制方式。

二、訂定媒介物之管制方式，並檢視其保管情形。

三、針對不同媒介物存在之環境，建置適度之保護設備或技術。

2 前項所稱環境，指第十四條所定各類設備、儲存媒體或媒介物之存放區域。

第 17 條

1 非公務機關為確實保護個人資料之安全，應對其所屬人員採取適度管理措施。

2 前項管理措施，應包括下列事項：

一、依據業務需求，適度設定所屬人員不同之權限，控管其接觸個人資料之情形，並定期檢視權限內容之適當性及必要性。

二、檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。

三、要求所屬人員妥善保管存有個人資料之媒介物，並約定保管及保密義務。

四、所屬人員異動或離職時，應將執行業務所持有之個人資料辦理交接，不得在外繼續使用，並應簽訂保密切結書。

第 18 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，使其明瞭個人資料保護相關法令之要求、所屬人員之責任範圍、各種個人資料保護事項之作業程序及應遵守之相關管理措施。

第 19 條

1 非公務機關為確保本計畫及處理方法之落實，應依其業務規模及特性，衡酌經營資源之合理分配，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。

2 前項檢查結果應向負責人提出報告，並留存相關紀錄，其保存期限至少五年。

3 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 20 條

1 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。

2 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。

3 前二項之軌跡資料、相關證據及紀錄，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

第 21 條

非公務機關應隨時參酌業務與本計畫及處理方法之執行狀況、社會輿情、技術發展及相關法規訂修等因素，檢討所定本計畫及處理方法，必要時予以修正；修正時，應於十五日內將修正後之本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。

第 22 條

1 非公務機關委託他人蒐集、處理或利用個人資料之全部或一部時，應對受託人依本法施行細則第八條規定為適當之監督。

2 非公務機關為執行前項監督，應與受託人明確約定相關監督事項及方式。

第 23 條

非公務機關業務終止後，其保有之個人資料不得繼續使用，應依下列方式處理，並留存相關紀錄，其保存期限至少五年：

一、銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

二、移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

三、其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

第 24 條

本辦法發布施行前，未訂定本計畫及處理方法之非公務機關，應依本辦法規定訂定，並於本辦法發布施行日起六個月內，將本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關或財團法人主管機關備查。

第 25 條

本辦法自發布日施行。

(○○公司名稱)個人資料檔案安全維護計畫或業務終止後個人資料處理方法(範本)

○○年○○月○○日訂定

壹、組織、規模及特性

一、行業特性：

□營造業　　□不動產開發業

□建築師事務所　　□公寓大廈管理維護公司

□都市更新業務財團法人　□其他經中央主管機關公告指定者

二、組織型態：事務所或聯合事務所、股份有限公司、有限公司或獨資(合夥)商號

三、資本額：新台幣○○○萬元整

四、處所地址：○○市○○區○○路（街）○段○號○○樓

五、代表人（負責人）：○○○(參考個人資料保護法第 50 條)

六、員工人數：（可記載一定範圍之人數）

貳、個人資料檔案之安全維護管理措施(計畫內容)

一、管理人員及資源

（一）管理人員：

1、配置人數：○人。(建議至少配置 1 名管理人員)

2、職責：負責規劃、訂定、修正與執行個人資料檔案安全維護計畫或業務終止後個人資料處理方法（以下簡稱本計畫或處理方法）等相關事項，並向負責人提出報告。

（二）預算：每一年新台幣○○萬元。（依實際狀況填寫）

（三）個人資料保護管理政策：遵循個人資料保護法關於蒐集、處理及利用個人資料之規定，並確實維護與管理所保有個人資料檔案安全，以防止個人資料被竊取、篡改、毀損、滅失或洩漏。

（四）本公司(商號)應將聯絡資訊（連絡窗口為：○○○，電話為：○○○○○○）揭示於本公司(商號)營業處所或公司（商號）

網頁，以提供當事人(客戶)表示拒絕接受行銷、個人資料事故諮詢服務及行使個人資料保護法第三條之權利聯絡使用。

二、個人資料之範圍

（一）特定目的：行政管理、不動產開發服務、建築管理都市更新、國民住宅事務、契約或類似契約或其他法律關係事務、信託業務、消費者、客戶管理與服務、人事管理、住宅行政。（類別：識別類、特徵類、家庭情形、社會情況、教育、考選、技術或其他專業、受僱情形、財務細節、商業資訊、健康與其他、其他各類資訊。請參考法務部「本法之特定目的及個人資料之類別」表格(個人資料保護法第 53 條)，若查無相對應之特定目的及個人資料類別，得自由敘述補充）

（二）個人資料：

1、本計畫之個人資料類型，不以消費者為限。

2、個人資料係指自然人之姓名、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、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

（三）依個資法第 51 條第 1 項規定，以下個人資料排除於本計畫之外：

1、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

2、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。。

三、風險評估及管理機制

（一）風險評估：

1、經由本公司(商號)電腦下載或外部網路入侵而外洩。

2、員工及第三人故意竊取、毀損或洩漏。

3、設備送修、遺失或被竊。

4、業務終止後個人資料未銷毀。

（二）管理機制：

1、定期進行網路資訊安全維護及控管。

2、落實教育訓練及管理稽核，並監督其業務之執行。

3、設備送修前或保存，應先備份或加密，避免非授權存取。

4、個資檔案使用期限已結束應銷毀。

5、○○。(註：倘經評估有其他風險管理機制，請自行增列。)

四、個人資料蒐集、處理及利用之內部管理措施

（一）告知義務：

1、直接向當事人蒐集個人資料時，應明確告知當事人下列事項：(1)本公司(商號)名稱。(2)蒐集目的。(3)個人資料類別。(4)個人資料利用之期間、地區、對象及方式。(5)當事人得 查詢或請求閱覽、製給複製本、補充或更正、刪除、停止蒐 集、處理或利用其個人資料之權利及申請程序。(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。

2、所蒐集非由當事人(或客戶)提供之個人資料，應於處理或利用前，向當事人告知下列事項：(1)個人資料來源。(2)本公司(商號)名稱。(3)蒐集目的。(4)個人資料類別。(5)個人資料利用之期間、地區、對象及方式。(6)當事人得查詢或請求閱覽、製給複製本、補充或更正、刪除、停止蒐集、處理或利用其個人資料之權利及申請程序。

（二）於告知當事人上述應告知事項後，獲得客戶書面同意，始得進行個人資料之合法蒐集、處理及利用。

（三）本公司（商號）要求所屬人員為執行業務而蒐集、處理一般個人資料時，應檢視是否符合個資法第 19 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，應檢視是否符合個資法第 20 條第 1 項但書情形。

（四）本公司（商號）於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。當事人（或客戶）表示拒絕接受行銷時，本公司(商號)應立即停止利用其個人資料行銷，並將拒絕情形通報（公司）彙整後再周知所屬各部門。

（五）內政部對本公司（商號）所屬行業為限制國際傳輸個人資料之命令或處分時，本公司（商號）應通知所屬人員遵循辦理。所屬人員於國際傳輸個人資料時，應檢視未受上開限制，及無個人資料保護法第 21 條 4 種例外情形，始得合法進行國際傳輸，並告知當事人其個人資料所欲國際傳輸之區域對資料接收方為下列事項之監督：1.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。2.當事人行使本法第 3 條所定權利之相關事項。

（六）當事人(客戶)請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，本公司（商號）應告知當事人行使上述權利之申請程序。受理申請時應確認申請人身份，申請文件有遺漏或欠缺，應通知申請人限期補正。如認有拒絕當事人行使上述權利之事由，應附理由通知當事人。當事人請求答覆查詢、提供閱覽個人資料或製給複製本時，如有收取__

_____必要成本費用者，應主動告知收費基準。上述申請程序，應依個資法第 13 條規定於處理期限內辦理完成。

（七）本公司（商號）於蒐集、處理或利用過程中，應維護個人資料之正確，有不正確時，應主動或依當事人之請求更正或補充之。

（八）經清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，除因執行職務或業務所必須或經當事人書面同意者外，應予刪除、停止蒐集、處理或利用該個人資料之處置，並留存記錄。

（九）本公司(商號)如有委他人（或他公司）蒐集、處理或利用個人資料時，應與受託者明確約定相關監督事項，至少應包含個資法施行明細第 8 條第 2 項所規定之各款事項，並定期確認其執行狀況。（註：如未委託他人則可刪除免予敘明）

五、事故之預防、通報及應變機制

（一）預防：

1、本公司(商號)員工或所屬之建築師如因其工作執掌而須輸出、輸入個人資料時，均須鍵入其個人之使用者代碼及識別密碼，同時在使用範圍及使用權限內為之。

2、非承辦之建築師或員工參閱契約書類時，應得公司（商號）負責人或經指定之管理人員之同意。

3、加強員工教育宣導，並嚴加管制。

（二）通報及應變：

1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向公司(商號)負責人通報，並立即查明發生原因及責任歸屬，及依實際狀況採取必要措施。

2、對於個人資料遭竊取之當事人（客戶），於事故查明後即時以書面通知使其知悉被侵害之事實、本公司(商號)已採取之處理措施及諮詢服務專線。

3、遇有達 1,000 筆以上之個人資料事故時，於發現後 72 小時內，以書面（格式如附件）通報○○市（縣）政府○○局（處）或財團法人主管機關。

4、針對事故發生原因研議改進措施，避免類似個人資料事故再次發生。

5、個人資料事故相關紀錄文件應妥善留存。

六、資料安全管理、資通訊系統、人員管理、環境及實體設備

（一）資料安全管理

1、訂定各類設備或儲存媒體之使用規範：

（1）個人資料檔案儲存在個人電腦者，應設置識別密碼、保護程式密碼及相關安全措施。

（2）定期進行電腦系統防毒、掃毒之必要措施。

（3）對於各類委託書、契約書件（含個人資料表）應存放於公文櫃內並上鎖，員工或所屬人員非經公司（商號）負責人或營業處所主管同意不得任意複製或影印。

2、設備送修前應備份或加密，避免設備送修或遺失被非授權取得個人資料。

3、設備或紙本，於報廢、汰換或轉作其他用途時，應採取適當防範措施，避免個人資料銷毀、轉移程序不當而洩漏個人資料。

（二）資通訊系統管理（註：如無，則免敘明）

因本公司（商號）所使用_____系統蒐集、處理或利用個人資料，且其資料庫保有個人資料數量達 5000 筆以上者，應採取下列措施：

（1）使用者身分確認及保護機制：(例如：建立帳號管理機制，並執行身分驗證管理，身分驗證資訊不以明文傳輸、密碼複雜度或帳號鎖定機制等)。

（2）個人資料顯示之隱碼機制：(例如：將身分證字號中間或末4碼以*標示，將姓名中間以○標示)。

（3）網際網路傳輸之安全加密機制：(例如：網站採用 https。電子郵件採用 TLS 、附件先加密再傳輸。檔案傳輸使用 sftp。個人資料之匯出檔案宜加密保護。)

（4）個人資料檔案及資料庫之存取控制與保護監控措施：(例如：網網站或資料庫之存取控制，宜採用最小權限原則。未使用之網站或資料庫等服務宜下架。)

（5）防止外部網路入侵對策：(例如：定期網站弱點掃描並修復弱點，實作注入避免、應用程式防火牆等。)

（6）非法或異常使用行為之監控與因應機制：(例如：網定期檢視系統相關日誌紀錄，或設置適當監控及異常行為預警機制。)

（三）人員管理

1、適度設定所屬人員使用個人資料之工作權限，並控管其接觸個人資料之情形，並依工作職務或人員異動調整工作權限。

2、各個資業務流程應指定管理人員，負責定期管理稽核各項個人資料檔案之安全管理措施。

3、本公司（商號）員工及所屬人員應妥善保管儲存個人資料之媒介物，並要求遵守個人資料內容之保密義務（含契約終止後）。(註:媒介物指存有個人資料之紙本、磁碟、光碟片等物品。)

4、職務異動或所屬人員與公司（商號）終止僱傭或委任契約時，其所持有之個人資料應辦理交接，並簽訂保密切結書。

（四）環境及實體設備安全

1、個人資料之資訊設備或紙本應置放於安全區域(如：門禁控管區域、機房、檔案室)，並設有監控設備(如：監視器、防盜系統)。相關進出管制簽名記錄、門禁記錄、影像攝影等記錄應妥善保管並嚴禁修改。

對於各類委託書、契約書件（含個人資料表）應存放於公文櫃內並上鎖，未經申請程序不得任意複製或影印。

2、資訊設備之攜入（例如新購硬碟）、攜出（例如送修、報廢），應透過申請程序經單位主管同意，並作成紀錄。

3、保存個人資料有安全之環境控管（溫、濕度管制、遠離火源、不斷電系統）。

七、資料安全稽核機制

（一）本公司(商號)定期(每半年至少一次)辦理個人資料檔案安全維護稽核，查察是否落實本計畫或處理方法各事項，針對不符合事項及潛在不符合之風險，應規劃改善措施，並確保相關措施之執行。執行改善與預防措施時，應依下項事項辦理：

1、確認不符合事項之內容及發生原因。

2、提出改善及預防措施方案。

3、紀錄查察情形及結果。

（二）前項查察情形及結果應載入稽核報告中，由公司(商號)負責人簽名確認。

八、使用記錄、軌跡資料及證據保存

所有個人資料之使用記錄、軌跡資料及證據，應至少留存五年。但法令另有規定或契約另有約定者，不在此限。

(註：本項請依實際情形說明公司（商號）如何保存紀錄、保存方式、保存期限、取得紀錄或證據之申請程序、保存期限屆滿之處理。)

九、認知宣導及教育訓練

（一）本公司(商號)每年進行個人資料保護法基礎教育宣導及教育訓練至少○次，使員工或所屬人員知悉應遵守之規定。前述教育宣導及訓練應留存紀錄。

（二）對於新進人員應特別給予指導，務使其明瞭個人資料保護相關法令規定、責任範圍及應遵守之相關管理措施。

十、個人資料安全維護之整體持續改善

本公司（商號）隨時依據業務與本計畫及處理方法之執行狀況，注意相關社會輿情、技術發展及相關法規訂修等事項，檢討所定本計畫及處理方法是否合宜，必要時予以修正；如修正，應於 15 日內將修正後之本計畫及處理方法報請主事務所所在地之○○市（縣）政府○○課（局）或財團法人主管機關備查。

十一、業務終止後之個人資料處理方法

針對個人資料之銷毀、移轉或刪除、停止處理或利用等作業，應規範其處理方式及應記載事項，並留存相關紀錄； 委託他人執行者，亦應遵守本項規定辦理。

（一）進行個人資料銷毀時，應記錄其銷毀個人資料之方法、時間、地點及證明銷毀之方式等欄位。

（二）進行個人資料移轉時，應記錄其移轉個人資料之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據等欄位。

（三）進行個人資料刪除停止時，應記錄其刪除、停止處理或利用之方法、時間或地點等欄位。

附件　個人資料事故通報及紀錄表

<table>
<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。

說明：配合內政部指定營建類非公務機關個人資料檔案安全維護管理辦法第九條規定非公務機關發生重大個人資料事故之情事者，應於七十二小時內將相關事項以書面通報各該主管機關，爰擬定「個人資料外洩通報表」之統一格式俾利非公務機關填報。