【授權聲明】

本程序書為安律國際股份有限公司(以下簡稱安律國際公司)，為服務公司客戶所訂定個人資料檔案安全維護計畫範本(以下稱本範本)，所有內容均由安律國際公司自行發展及擁有合法之著作及版權得授權使用者使用本範本。

## 本範本之目的僅供公司客戶（下稱使用者）參考，安律國際公司授權凡經安律國際公司同意而取得本範本的使用者得利用本範本並進行編修，惟前開利用及編修僅限使用者公司基於訂定內部規章、建立內部制度或內部教育訓練之目的。

## 安律國際公司禁止使用者對第三人使用或提供本範本/編修本，禁止範圍包括但不限於將本範本/編修本換價或以之用於行銷、推廣業務等商業行為。

## 安律國際公司對使用者參考本範之行為聲明免責，使用方應自行評估並自行承擔使用本範本所致一切影響。

# 安全維護計畫使用說明

## 標示說明

本範本內，由於使用者的組織大小及架構或有不同，因此本範本標示以下顏色提醒使用者進行修改或替換。

███ 黃色標記: 黃色標記為指派的人員角色或小組的名稱，使用者可依據自己組織的情況調整。

███ 藍色標記: 用於標示「個資管理代表」，個資管理代表為組織內管理個人資料保護事宜最高的主管，使用者可以依據自己組織內最個資管理最高主管的名稱置換藍色的標記。

███ 綠色標記: 綠色標記為設定值(例如: 每年執行一次)，此類設定值，使用者可以依據自己的情形或決策進行調整。

## 適用對象

個人資料檔案安全維護計畫 (以下稱『安全維護計畫』)，係依據中華民國數位發展部 (以下簡稱數發部) 於112 年10 月12 日頒布的『數位經濟相關產業個人資料檔案安全維護管理辦法』而編訂的個人資料檔案安全維護計畫，適用對象為以下行業:

|  |  |
| --- | --- |
| 行政院主計總處行業統計分類分類編號及行業名稱 | 適用之行業 |
| 4871電子購物及郵購業 | 從事以網際網路方式零售商品之行業（不含電視、廣播、電話等其他電子媒介及郵購方式）  |
| 582 軟體出版業 | 軟體出版業  |
| 620 電腦程式設計、諮詢及相關服務業 | 電腦程式設計、諮詢及相關服務業  |
| 6312資料處理、主機及網站代管服務業 | 從事代客處理資料、主機及網站代管以及相關服務之行業（不含線上影音串流服務）  |
| 639 其他資訊服務業 | 其他資訊服務業  |
| 6699未分類其他金融輔助業 | 第三方支付服務業（不含其他金融輔助業）  |

## 個資法管理應辦事項整理



個資法中規定個資的蒐集、處理、利用、停止/刪除等管理生命週期中的應執行及合法的要求，數發部的管理辦法第9條、第10條及第11條也明確規範公司應建立執行的內部程序以及應實施的管理措施，公司應依據個資法及主管機關管理辦法建立完善且合於法律規定的管理制度並據以執行。

## 定期執行之相關作業

### 規劃年度個資管理作業時程

安全維護計畫需規劃

個人資料盤點作業

個人資料風險評估

年度內部稽核

##### 等之相關作業時程，並通知各部門配合執行。

### 年度教育訓練

教育訓練小組於每年度一月依據需求規劃該年度之教育訓練計畫，並實施辦理相關訓練。

由教育訓練小組發佈相關訓練時程及規劃，各部門應依循相關規劃配合參與。

### 個資盤點暨風險評估

各部門應每年定期執行個資盤點作業，以界定保有個資之範圍。

完成個資盤點作業後，另須針對該個資檔案進行後續風險評估作業。

### 內部稽核

內部稽核小組應於每年一月規劃視需求規劃該年度稽核計畫，並依據分工及獨立性原則規劃組成績合小組。

於內部稽核時，針對執行內容與程序書規定進行查檢。

內部稽核結果，若有不符合事項需列出，並請受稽核部門進行矯正作業。

針對受稽部門提出之矯正改善作業，由內部稽核部門進行檢視及追蹤，以完善相關改善作業。

### 個資保護執行作業報告

每年至少一次，由個資管理代表召集個資管理小組執行年度個資保護執行作業報告，由公司相關作業執行人員及個資管理小組進行各部門個資保護及全體個資保護作業之成果報告，並統計執行紀錄資訊後提供給個資管理小組進行彙整，以確保所有之個人資料檔案安全維護計畫執行結果均符合公司之需求。

安律支付

個人資料檔案安全維護計畫

(參考範本)

 中華民國 112 年 12 月 1日修訂

安律支付股份有限公司

使用者可依據自我的需求進行調整 (記得移除公司名稱及Logo)

**目　次**

[壹、 個人資料保護管理政策 1](#_Toc153808750)

[一、 政策制定依據 1](#_Toc153808751)

[二、 個資保護政策 1](#_Toc153808752)

[三、 個人資料保護聯絡窗口 2](#_Toc153808753)

[四、 政策適用範圍 3](#_Toc153808754)

[五、 個人資料保護政策管理作業 3](#_Toc153808755)

[貳、 個人資料管理組織 5](#_Toc153808756)

[一、 個人資料管理組織結構 5](#_Toc153808757)

[二、 組織職掌 6](#_Toc153808758)

[三、 組織成員說明 9](#_Toc153808759)

[參、 適用法規盤點程序 10](#_Toc153808760)

[一、 執行目的 10](#_Toc153808761)

[二、 執行人員 10](#_Toc153808762)

[三、 法規遵循 10](#_Toc153808763)

[四、 檢視修訂法令及其他規範 10](#_Toc153808764)

[五、 登載法令及其他規範 10](#_Toc153808765)

[肆、 個人資料作業管理程序 11](#_Toc153808766)

[一、 個人資料蒐集管理 11](#_Toc153808767)

[二、 特定目的及類別 11](#_Toc153808768)

[三、 個人資料處理及利用管理 11](#_Toc153808769)

[四、 個人資料行銷利用 12](#_Toc153808770)

[五、 個人資料保存管理 13](#_Toc153808771)

[六、 資料正確性維護 13](#_Toc153808772)

[七、 國際傳輸 13](#_Toc153808773)

[八、 特種個人資料之蒐集、處理、利用限制 14](#_Toc153808774)

[九、 個人資料封裝及傳遞 14](#_Toc153808775)

[十、 個人資料銷毀管理 14](#_Toc153808776)

[十一、 最小蒐集原則 15](#_Toc153808777)

[十二、 去識別化 15](#_Toc153808778)

[十三、 個人資料委外蒐集、處理、利用管理 15](#_Toc153808779)

[十四、 個人資料事件通報 16](#_Toc153808780)

[伍、 個人資料委外管理程序 17](#_Toc153808781)

[一、 確認項目 17](#_Toc153808782)

[二、 確認受委託者就施行細則第12條第 2項應採取之必要措施 17](#_Toc153808783)

[三、 規範複委託者，其約定之受託者 20](#_Toc153808784)

[四、 違反通知 20](#_Toc153808785)

[五、 本公司如對受委託者有保留指示者，監督保留指示之事項 21](#_Toc153808786)

[六、 委託關係終止或解除 21](#_Toc153808787)

[七、 監督之方式 22](#_Toc153808788)

[陸、 當事人權利行使管理程序 24](#_Toc153808789)

[一、 本公司個資作業當事人權利請求作業流程 24](#_Toc153808790)

[柒、 個人資料之風險評估及管理機制 27](#_Toc153808791)

[一、 個人資料盤點作業程序 27](#_Toc153808792)

[二、 風險評估作業 30](#_Toc153808793)

[三、 風險管理作業 32](#_Toc153808794)

[捌、 事故之預防、通報及應變機制 34](#_Toc153808795)

[一、 個人資料事件處理流程 34](#_Toc153808796)

[二、 個人資料事件通報管理 35](#_Toc153808797)

[三、 個人資料之事件懲處管理 36](#_Toc153808798)

[玖、 資料安全管理及人員管理 37](#_Toc153808799)

[一、 資料安全防護措施 37](#_Toc153808800)

[二、 資料存取安全措施 41](#_Toc153808801)

[三、 資料存放安全措施 42](#_Toc153808802)

[四、 資料備份安全措施 44](#_Toc153808803)

[五、 人員聘僱管理 45](#_Toc153808804)

[六、 機密維護責任 46](#_Toc153808805)

[七、 人員資訊作業注意事項 47](#_Toc153808806)

[壹拾、 設備安全管理 48](#_Toc153808807)

[一、 個資處理設備清查 48](#_Toc153808808)

[二、 設備安全需求 49](#_Toc153808809)

[壹拾壹、 認知宣導及教育訓練 52](#_Toc153808810)

[一、 訓練需求評估 52](#_Toc153808811)

[二、 訓練計畫 53](#_Toc153808812)

[三、 訓練執行 53](#_Toc153808813)

[四、 訓練結果維持 53](#_Toc153808814)

[五、 成效評估與計畫修正 54](#_Toc153808815)

[壹拾貳、 資料安全稽核機制 55](#_Toc153808816)

[一、 稽核人員 55](#_Toc153808817)

[二、 稽核管理 55](#_Toc153808818)

[三、 稽核計畫 56](#_Toc153808819)

[四、 稽核範圍 56](#_Toc153808820)

[五、 稽核頻率 57](#_Toc153808821)

[六、 稽核方法 57](#_Toc153808822)

[七、 稽核紀錄與報告 57](#_Toc153808823)

[八、 稽核改善與追蹤 58](#_Toc153808824)

[壹拾參、 個人資料安全維護之整體持續改善 59](#_Toc153808825)

[一、 程序目的 59](#_Toc153808826)

[二、 檢查 59](#_Toc153808827)

[三、 持續改善 60](#_Toc153808828)

[附件一、個人資料保護管理小組組織名單 61](#_Toc153808829)

[附件二、個資保護適用法規一覽表 62](#_Toc153808830)

[附件三、新個資蒐集前查檢表 63](#_Toc153808831)

[附件四、新個資利用前申請書 65](#_Toc153808832)

[附件五、個人資料權利行使申請書 67](#_Toc153808833)

[附件六、個人資料盤點表(另提供 Excel 檔) 69](#_Toc153808834)

[附件七、風險處理計畫(提供 Excel 表) 70](#_Toc153808835)

[附件八、教育訓練成果報告表 71](#_Toc153808836)

[附件九、稽核查檢表暨工作底稿 73](#_Toc153808837)

[附件十、稽核報告書 77](#_Toc153808838)

[附件十一、矯正預防單 78](#_Toc153808839)

[附件十二、銷毀申請單 79](#_Toc153808840)

[附件十三、個資事件通報單 80](#_Toc153808841)

# 個人資料保護管理政策

## 政策制定依據

安律支付股份有限公司（以下簡稱本公司）依據個人資料保護法、個人資料保護法施行細則及本公司個人資料保護之相關規定，以及主管機關個人資料檔案安全維護管理辦法，制訂個人資料保護管理政策(以下簡稱本政策)。

## 個資保護政策

僅於合法、合規前提下蒐集、處理、利用個資

個人資料為本公司為了服務客戶、消費者而蒐集、處理、利用的資訊。本公司僅在合於我國個人資料保護相關法令、主管機關規定的前提下蒐集、處理及利用個人資料。任何違反法令或主管機關規定的活動應立即停止，有違反法令或主管機關規定風險的活動應於風險降低或消除後才得執行。

### 尊重隱私原則

所有公司的業務及活動均以保護、尊重客戶、消費者的隱私權為最高指導原則，合法及安全的進行個人資料保護是對客戶及消費者的權益保障及基本的尊重，任何侵犯客戶或消費者隱私的流程與業務方式必須立即改善。公司的業務及活動均須採對於隱私權衝擊最小的方式進行。

### 資料安全處理原則

凡客戶資料與營運資訊，必須建立對應的安全處理環境，確保資料的安全後才得進行商業的運行及資料的利用。

資訊系統及作業流程應確保個人資料之正確性，並符合資訊安全要求之機密性、完整性及可用性。

持續維運個人資料安全維護計畫，確保個人資料檔案的安全。

### 最小蒐集原則

所有對於個人資料的蒐集，均以最小蒐集為原則，非必要的個人資料，不予蒐集。業務流程設計以隱私保護為優先，應考慮不蒐集個資仍得以進行業務的方式，減少對個人資料的蒐集。

### 去識別化與匿名化

系統設計及流程設計，應考慮盡可能進行資料的去識別化或匿名化處理，以降低資料的風險性。無須識別當事人之個資利用，應將個資去識別化。

### 最小保存原則

個人資料的留存，應訂定其保留之期限，超過法定或業務目的保存期限的個人資料，均應以去識別方式保存或予以刪除。

### 資料存取管控原則

系統設計及服務流程設計，均需建立並留存足夠的資料存取的紀錄，確保對於資料利用的可歸責性，以及建立對於資料利用的監督與管理。 資料庫等大量資料存放設備，於接受其他系統介接時，開通前應審查該系統的資料使用目的、範圍及資料管控能力，確保符合本資料管控原則。

## 個人資料保護聯絡窗口

本公司設立個人資料保護聯絡人進行個人資料保護管理事宜的處理及個人資料檔案的安全維護。

相關於本公司個人資料保護事宜及當事人權利行使的事項，請洽本公司個資保護聯絡人。

 個人資料保護聯絡人

 姓名: ○○○ 先生

 電話: 02-2300-1234

 Email: privacy@abcooo.com.tw

## 政策適用範圍

本公司之個人資料保護政策適用於管理或使用本公司個人資料之所有人員，包括員工、委外人員、廠商以及其他因本公司營運或合作關係得以接觸本公司個人資料或相關系統之人員。

## 個人資料保護政策管理作業

### 政策之核准

本政策應由個資管理小組進行訂定與修正，並由本公司授權之個資管理代表核定。

### 政策之執行

本政策於個資管理代表核定後公布實施，所有本公司內與個人資料保護相關之作業，均應遵循本政策。

本政策之執行由個資管理小組針對綱領性質進行規劃，並由各部門執行政策之推行。

個資專人應透過本計畫稽核機制定期進行對於政策遵循的查核，以確保政策及本計畫之執行成效，相關執行成效應呈報個資管理代表。

### 政策修正與調整

個資專人應於至少每年或於個人資料保護法相關法規有重大變化後審視及修訂本政策，以確保本政策之適用性。

政策公告及傳達方式

個人資料保護政策，對內應透過內部公告方式進行傳達，個資相關訓練課程均應含括個資保護政策以及本計畫內容。

對外應透過適當管道如公司網站或其他客戶或消費者能觸及的方式進行個人資料保護政策的傳達，委外作業如涉及個人資料的蒐集、處理及利用者，應以適當方式傳達本公司個人資料保護政策，並應於委外合約內進行相關政策遵循要求。

# 個人資料管理組織

本公司依據個人資料相關法令及主管機關管理辦法配置管理人員及相關資源，組成個人資料管理組織。

## 個人資料管理組織結構

### 個人資料管理組織

本公司設置「個人資料保護及管理推動小組」（以下簡稱個資管理小組），由資訊安全長擔任個資管理代表，組織設置

個人資料保護聯絡窗口

預防/通報/應變小組

教育訓練小組

稽核小組

個資管理小組

個資管理代表 資訊安全長

個人資料保護

聯絡窗口

預防/通報/應變小組

教育訓練
小組

稽核小組

個資管理小組執掌

訂定及修正個人資料保護管理政策

訂定及修正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「安全維護計畫」)

依據個人資料保護管理政策執行安全維護。

各功能分組依據分組執掌進行個人資料保護管理業務。

各部門個資管理執掌

經個資管理小組指派後，本公司各部門，應設置個資專人依各部門所保有之個人資料種類不同，進行個人資料保護作業，個資專人執掌如下說明：

執行各部門個人資料檔案安全維護計畫。

部門內個人資料保護管理之規劃及執行。

個人資料保護法令規定諮詢。

個人資料保護事項協調聯繫。

部門內個人資料損害預防及危機處理應變之通報。

個人資料保護自行查核及本公司個人資料保護政策之執行。

## 組織職掌

### 個資管理小組

管理代表

本公司授權由本公司資安長擔任個資管理代表。

提供部門充分人力及資源確保個人資料保護管理組織之運作。

指派個資管理小組成員規劃及執行個資檔案安全維護計畫。

指派個資管理小組成員規劃及執行個資保護相關內部程序。

核准個人資料保護管理政策及相關個人資料管理程序及管理辦法。

確認個人資料安全內部稽核結果及改善結果。

個人資料保護聯絡窗口

依管理辦法規定設置個人資料保護聯絡窗口

由個資管理代表指派OO部門OO擔任個人資料保護聯絡窗口。

接受個人資料當事人行使其個人資料相關權利。

接受個人資料當事人、客戶或消費者提出個人資料處理相關申訴與諮詢。

重大個人資料事故之客戶或消費者聯繫單一窗口，重大個人資料事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及非公務機關正常營運或大量當事人權益之情形。

預防/通報/應變小組

由個資管理代表指派AAA 部門OOO為小組組長，並由小組組長視需求指派相關組員。

負責個人資料事故之預防、應變及通報處理作業。

研議及執行個資外洩緊急應變計畫暨作業處理程序。

依據本計畫進行個資事故之通報。

進行個人資料事故後對於受影響客戶或消費者之通知。

查明個資事故之發生原因及處理情形並向個資管理代表報告。

教育訓練小組

由個資管理代表指派CCC 部門OOO為小組組長，並由小組組長視需求指派相關組員。

本公司個資教育訓練名單及紀錄之彙整。

負責個人資料保護及本計畫實施相關教育訓練執行。

規劃及修訂教育訓練計畫。

指派協調執行教育訓練人員。

評估教育訓練之成效。

完成教育訓練作業後向個資管理代表報告稽核結果。

稽核小組

由個資管理代表指派DDD 部門OOO為小組組長，並由小組組長視需求指派相關組員。

負責本公司個人資料安全維護計畫之內部稽核作業。

規劃、管理及執行稽核計畫。

組織執行稽核人員。

執行稽核教育訓練。

完成稽核作業後向個資管理代表報告稽核結果。

### 各部門職掌

個資專人

各部門皆需設個資專人至少一人，由個資管理代表任命。

個資專人之執掌為

###### 維護部門相關個資管理程序及辦法。

###### 進行年度之個人資料風險評估及風險管理。

###### 維持本公司資料安全及設備之安全。

###### 執行本公司規定之資訊安全要求。

###### 接受當事人權利行使作業申請。

###### 持續改善本公司之個人資料管理流程。

###### 部門內部個人資料法律問題諮詢窗口。

部門聯絡人

各部門設置聯絡人一名，由個資管理代表任命；可視需求併入個資專人職責。

個資保護事項相關協調聯繫。

與本公司各部門及各部門溝通個人資料保護相關事宜。

## 組織成員說明

本公司個人資料保護管理組織之成員之名單請詳見**附件一**。

# 適用法規盤點程序

## 執行目的

個人資料保護法及相關配套法令及規定會因為社會變遷及實際施行狀況而進行修訂或增補，個人資料保護委員會及各目的事業主管機關、縣市政府均得針對個人資料保護法提出對應規定或指引做法，本公司為確保公司執行之作業能遵循法令規範並確保個資當事人之權益，訂定此程序。

## 執行人員

由本公司法務相關部門及各部門個資專人執行相關法規的蒐集及更新，並進行法規之蒐集及彙整清冊。

## 法規遵循

各部門個資專人，應於法規盤點後，透過認知宣導、人員訓練、資訊公布或其他適當方式使公司內人員知悉法規之要求並確實遵守。

## 檢視修訂法令及其他規範

個資專人為維持個人資料保護法及其他相關法令規範為最新之狀態，應定期檢視或於法律修訂公告後進行法規更新狀況之檢查。

於本公司各部門業務項目、範圍有新增變動時，亦必須重新檢視法規盤點清冊之內容。

## 登載法令及其他規範

個資專人應將盤點結果更新於「個資保護適用法規一覽表」中並提供於本公司各部門知悉，格式如**附件二**。

# 個人資料作業管理程序

個人資料自公司蒐集開始，就必須符合個人資料保護法的規定進行合法蒐集，除依循蒐集特定目的，進行適當的安全維護外，利用也需要在特定目的的必要範圍內，本公司訂定本內部程序，規範所有公司業務執行而蒐集、處理、利用的個人資料均符合法令規定及本公司個人資料保護政策。

## 個人資料蒐集管理

個人資料新蒐集，在公司進行個人資料的蒐集前，必須進行合法性的檢視，確保所有的蒐集行為均符合法令規定及合於本公司個資保護政策。個人資料蒐集的方式，包含直接蒐集及間接蒐集(個資取得非直接由個資當事人取得)。

個人資料新蒐集前應檢查蒐集合法性並由預計蒐集部門，或主要負責部門個資專人填具「新個資蒐集前查檢表」(如**附件三**)，經部門主管核准後，呈報個資管理代表進行核准，並於執行蒐集後一個月內更新「個人資料盤點表」 (**附件六**)。

個資專人及各部門資訊管理人員應進行或協助蒐集作業之監督，確保所有蒐集的作業均符合「新個資蒐集前查檢表」核准之蒐集方式及範圍。

## 特定目的及類別

個人資料保護法規範蒐集、處理、利用個人資料，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。(個資法第 5 條)，本公司進行個人資料的蒐集、處理、利用均須符合僅在特定目的必要範圍內。並應依據個資法第 8 條進行告知。(蒐集之目的與資料的類別)

## 個人資料處理及利用管理

間接蒐集得到的個人資料應特別注意其資料來源的合法性，本公司不應處理或利用未確認來源合法性的個人資料。

各部門個資專人應確認所處理的資料均符合「新個資蒐集前查檢表」中的資料項目，如果實際蒐集內容有超出或差異的部分，應向申請人說明並請該申請人及相關部門、技術部門修正，未符合法令或申請核准內容而得的蒐集內容應予以刪除，或於修正完成後使用。

在個人資料處理及利用過程如發現處理不合於個人資料保護法蒐集要件所取得之個人資料，或不合於特定目的之處理作業，應立即停止該資料的處理及利用，並呈報個資管理代表且須提出對於該資料的刪除及後續矯正作業。

個人資料新利用作業前，包含本公司因業務需求使用本公司既有保管及持有之個人資料，利用前應檢查利用之合法性並由各業務承辦人員填具「新個資利用前申請書」之表單(如**附件四**)，申請書經個資專人核准後，呈報個資管理代表審查核准。

本公司各部門權責主管應對個人資料利用的行為超出範圍時，應予以糾正，並提出矯正計畫避免事件再次發生。

個人資料之保管人或使用人調離職務時，應將所保管個人資料(電子檔案/紙本)交付權責主管或指定之交接人員，並更新盤點表後通知各部門個資專人備查。

個人資料之保管人及使用人於處理及利用個人資料過程中應注意確保其正確性及完整性。

## 個人資料行銷利用

個人資料如利用於行銷之目的，應進行

於蒐集時明確告知資料將利用於行銷，及其方式。

間接取得的個人資料，應於首次行銷利用時併同告知(進行個資法第 8 條應告知的內容)

### 提供拒絕行銷的方式

本公司蒐集的個人資料如果利用在行銷的目的上，應提供客戶或消費者適當的拒絕行銷管道及方式(例如透過 Email 或其他方式)，當客戶或消費者表示拒絕接受行銷者，應立即停止利用其個人資料於行銷。

## 個人資料保存管理

### 部門個資專人應負責查詢相關法律對於資料保存最小年限及保存最長年限之要求。

### 個人資料及蒐集相關告知或當事人同意證據之紙本或電子資料、電子形式軌跡資料(含應用系統及資料庫之軌跡資料、網路設備之異常軌跡資料等)，如無其他法令限制，應至少保存五年，以確保相關證據於個資法損害賠償請求權時效內均能完整提出。

個人資料的保存應與蒐集之目的有合理的關聯，並在特定目的消失後主動或依當事人請求進行刪除。

## 資料正確性維護

### 本公司應維持個人資料的正確性，並主動或依據當事人請求更正或補充。

### 資料正確性有爭議者，但因本公司執行業務所必須者，經當事人書面同意，應註明其爭議。

### 本公司更正或補充個人資料後，應以適當方式通知提供利用的對象。

## 國際傳輸

本公司如涉及將個人資料進行國際傳輸時，應告知當事人以下事項，並對於跨國傳輸的接收方進行監督:

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。

當事人行使本法第三條所定權利之相關事項。

### 如本公司需進行國際傳輸時，應檢查是否主管機關有規定國際傳輸的限制，並取得個資管理代表之核准。

## 特種個人資料之蒐集、處理、利用限制

本公司有關病歷、醫療、基因、性生活、健康檢查及犯罪前科等特種個人資料，非有其他法令明文規定，不得蒐集。

如需蒐集特種個人資料，各部門業務承辦人員應於經權責主管核准後向個資管理代表提出，由個資管理代表核決後始得蒐集、處理或利用特種個人資料。管理代表於核准該資料的蒐集、處理、利用事宜，應同時核准對於特種個人資料的資料安全保護方式。

## 個人資料封裝及傳遞

個人資料實體形式封裝應由各部門承辦人員封裝於傳遞信封內，外觀上不得標示其他足以顯示個人資料內容之註記。

個人資料於傳遞前應填寫簽收紀錄，並記錄相關傳遞細節以供日後查閱。

個人資料實體形式之傳遞，應依規定進行密件處理。

個人資料之電子形式傳遞，個人資料應以適當方式進行技術加密後傳送。

## 個人資料銷毀管理

為防範個資文件外流，紙本個人資料若有超過保存期限，不予保留而須進行銷毀時，應由部門業務承辦人員填寫「銷毀申請單」，經權責主管核准後，依本公司銷毀文件相關規定進行銷毀。

送至本公司以外銷毀之實體形式個人資料，須派專人參與運送並全程監督銷毀過程，留存相關紀錄並附於「銷毀申請單」以供備查。

「銷毀申請單」(**附件十二**)應由各部門個資專人保存至少五年。

## 最小蒐集原則

本公司對個資蒐集應以最小蒐集為原則，僅蒐集必要的個人資料欄位，有替代的方式且對當事人隱私衝擊較小者，應以衝擊性較小的方式進行個人資料的蒐集。且無須識別當事人者應以去識別化方式為之。

## 去識別化

本公司利用個資，如無須識別當事人者，應以個資去識別化方式為之蒐集、處理及利用相關資料。藉由代碼替換、刪除或隱藏部份個資欄位，使該個資紀錄無法直接識別當事人。

## 個人資料委外蒐集、處理、利用管理

### 本公司如需委由委外部門進行蒐集、處理、利用作業，應於委外事項進行前與該受委託部門進行委外作業的簽約。

### 本公司應依個人資料保護法相關規定對於個人資料委外作業進行監督。

### 本公司應要求受委託部門，定期或於需要時針對提供受委託之個人資料業務執行報告，並將報告呈報個資管理代表。

### 本公司應定期或於需要時針對受委託部門進行稽核，以確保所有的個人資料委託處理之作業均符合本公司之要求。

### 委外作業結束，本公司各業務部門應監督受委託部門返還或銷毀本公司已交付之個人資料，以確保個人資料之委外作業安全。

詳細之作業流程依本文件**伍、個人資料委外管理程序**之規範進行。

## 個人資料事件通報

本公司人員發現個人資料疑似洩露、遺失或遭竄改等異常現象，應立即通報各部門個資專人。

# 個人資料委外管理程序

依據個資法第4條、施行細則第7、8條規定，本公司於執行委外作業時應依本程序進行確認，並於委外過程中善盡監督之責任，委外作業得包括以下事項:

## 確認項目

確認受委託者知悉蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

委外業務承辦人員應以合約條款或書面確認方式，確認受委託者知悉本公司委託蒐集、處理或利用之個人資料。

範圍：本次委託作業中包含蒐集、處理、或利用那些個人資料項目。(如:姓名、電話、地址、身分證字號等)

類別：本次委託作業中包含蒐集、處理、或利用那些個人資料類別。(參考個資法法定類別列表)

特定目的：本次委託作業中蒐集的特定目的，或於委託處理、利用時告知本公司原蒐集個資的特定目的。(用於規範受託部門於蒐集、處理、利用個人資料時不超出特定目的)

期間：委託蒐集、處理、利用個資的期間。(此期間可能小於整體委託契約之契約有效期間)

本公司所涉及個人資料蒐集、處理、利用之委外作業，如需簽訂合約時，均須經由各部門個資專人確認其合約項目是否符合本委外管理程序要求，並經個資管理代表進行確認後始得進行該委外作業。

## 確認受委託者就施行細則第12條第 2項應採取之必要措施

委外業務承辦人員應於受委託者接觸本公司個人資料或開始進行個人資料蒐集前，確認該受委託者已採取適當安全之必要措施：

於合約中載明要求受委託者應依據個資法施行細則第12條第2項進行適當之安全維護措施，以及下列項目：

本公司對於受委託者之適當安全維護措施具體要求或條件。

適當安全維護措施定期檢核的頻率及方式(方式可能為要求受委託者定期繳交報表)。

如無法通過本公司對於受委託者的適當安全維護檢核，本公司有權解除委外合約，受委託者並應賠償本公司因此產生之損失。

如需要，本公司得進行受委託者之稽核作業或委由第三方進行稽核，以確保受委託者已進行適當安全維護措施，受委託者不得拒絕，並應支付稽核作業所需之費用。

於受委託者開始進行作業前視情況確認已實施適當安全維護措施之證明，建議該證明為(選擇其中一項即可)

各項要求之受委託者已執行之證據 (程序書、執行紀錄等)。

第三方公正部門出具之證明(如: ISO 27001、ISO 27701, BS 10012 證照等)。

本公司進行受委託者稽核之結果。

其他足資證明之文件(含保密切結)。

以上之證明，應於受委託者開始進行作業前，由委外作業承辦人員蒐集並留存紀錄，該證據並應經過各部門個資專人進行確認，必要時得請求本公司資訊管理部門進行技術性確認。

委外合約中應載明定期檢查適當安全維護措施之頻率及方式，並依其方式定期檢查並留下紀錄，合約中並應載明，無法通過本公司檢核該適當安全維護措施者，本公司可依規定立即終止或解除該委外合約。

如受委託者未能通過本公司對於適當安全維護措施之檢核，應

於合約簽訂前，應暫緩該合約之簽訂。

於合約簽訂後，委外作業開始執行前，應暫停該作業之啟動，並要求受委託者提出改善的時程及方式，如無法達成，應依合約條款逕行解約。

於合約簽訂後，委外業務執行中，應要求受委託者暫停該作業之執行，要求受委託者提出改善作業及矯正預防計畫，並依據合約條款進行相關作業因暫停而遲延之賠償。

外部稽核作業

如需要進行外部稽核以確認受委託者已進行適當安全維護措施，本公司應注意

稽核人員得為或包括

本公司各部門之個資專人。

本公司法律諮詢顧問人員

本公司資訊技術人員或外部技術人員

應建立稽核計畫，稽核查檢表設定內部對於通過稽核之標準條件，並於稽核前通知受委託者，以確保受委託者做好受稽核準備。

於稽核時應紀錄稽核發現之不符合項目，並做成稽核紀錄，該紀錄並應經過受委託者之負責人簽署確認。

如發現不符合事項，應要求受委託者提出矯正預防措施，並提出改善計畫及時程，必要時，得再次到現場進行稽核。

所有受委託者之矯正預防措施、改善計畫應取得稽核人員之確認後結案。

## 規範複委託者，其約定之受託者

本公司可依據各部門需求，與委託者簽訂合約或相關協議時，載明受委託方需經由本公司同意後始可進行再轉包給複委託對象；若較為敏感性之個人資料，則可另訂為禁止受委託方禁止進行複委託之行為等之內容，以避免無法監督到複委託之對象，或衍生其他的風險。

## 違反通知

確認受委託者或其受僱人違反個資法、其他個人資料保護法律，或其法規命令時，應向本公司通知之事項及採行之補救措施。

根據個人資料保護法第12條，本公司於發生個資事故時須於查明後通知當事人，如受委託者或其受僱人違反個資法或相關法令，或本公司之委託合約時，應規範受委託者向本公司通知及採行補救措施包括：

應於委外合約中載明

受委託者及其所有與本公司委外業務相關人員均應接受個人資料保護法及相關法令之訓練，以及了解本公司委外業務之要求。業務承辦人應定期確認所有受委託者人員狀態，以確保所有人員均知悉法令及本公司委外合約之規定或需求。

要求受委託者訂定於違反個資法法令及本公司委外合約時之處理程序，該程序必須包括：

受委託者處理專責人員指派。

應於事故發生後24小時內通知本公司業務承辦人員。

預擬補救措施之執行方式、資源及人力。

於事故處理完畢前，定期通知事故處理進度的頻率及方式。

如受委託者發生個人資料違法或違反本公司合約條款之事故，本公司得於事故處理完畢後即終止合約，未完成部份，另覓廠商完成。如受委託者無能力或因受委託者之故未能進行補救措施者，本公司得將委託其他部門進行該補救措施，受委託者並應支付該衍生之費用。

## 本公司如對受委託者有保留指示者，監督保留指示之事項

應於委外合約中要求

明確載明本公司對於受委託者之保留指示事項。

要求受委託者定期回報本公司要求保留指示之事項辦理狀況。

要求受委託者以書面方式或其他本公司事前同意方式取得本公司對於保留指示事項之同意，並留存相關紀錄。

留存相關受委託者請求指示及本公司指示紀錄。

定期或不定期對於受保留指示事項辦理狀況進行抽檢或稽核。

## 委託關係終止或解除

委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

本公司委外作業承辦人員應進行：

於合約中載明

受委託者應維持接受本公司個人資料之個人資料交付清冊，內容應包括：

個人資料的內容說明，個人資料項目、範圍及數量。

使用之載體及交付之方式。

日期、時間。

本公司交付人員及受委託者之收受人。

相關交付及接受之證明(例如簽名、簽收單據等)。

受委託者對於該交付資料的後續處理方式說明(包括複製、儲存、轉換等作業及可能產生之資料軌跡)

受委託者應定期清查並更新該資料清冊，確保其內容為最新，並定期交付給本公司委外業務承辦人員。

於合約終止或到期前一個月，得依據個人資料交付清冊訂定個人資料刪除之計畫，並取得本公司委外作業承辦人員之同意。

於合約終止或到期時交付個人資料刪除之清冊，其中包括：

原接收清冊之編號、範圍、項目及數量。

受委託者儲存的方式及數量清查結果。

受委託者進行的刪除方式及其刪除結果。

要求受委託者於刪除後提供由該組織簽署之切結書，切結受委託者未留存本公司交付之個人資料以及載明違反切結事項所應承擔之賠償責任，並經由本公司同意該切結內容。

如受委託者因合理之理由而無法刪除或需保留本公司所交付之個人資料，應向本公司委外作業承辦人提具申請及未刪除個資清冊、保留時間及方式，於取得本公司核准後留存及進行後續合約解約、終止作業。

## 監督之方式

委外業務承辦人應於合約簽署前，確認以下監督方式

監督定期查核的頻率。

監督的方式，以下為建議的監督方式

要求受委託者於每月(或其他頻率)繳交服務報告書內容時，交付個人資料安全維護狀況說明文件，其中包括本程序內之各項要求內容及異常或例外狀況說明。

由本公司人員定期進行文件、遠端或現場查核方式進行監督作業並留存紀錄。

監督之紀錄

委外業務承辦人員應定義監督紀錄的方式、內容要項及其保存方式。

監督之管理

###### 應定義執行監督之人員及其角色、權責。

###### 監督人員於發現不符合事項後之處理方式。

# 當事人權利行使管理程序

## 本公司個資作業當事人權利請求作業流程

權利請求申請

個資聯絡窗口或各部門個資專人負責當事人個資權利請求申請，本公司人員接受到相關請求，由個資專人確認後，進行相關權利申請之受理作業。

回應請求申請

各部門個資專人於收受個人資料當事人行使權利申請作業後，依個人資料保護法之要求回應當事人之申請。

當事人權利

依個資法第3條之規定，當事人就以下事項，可向本公司行使其權利:

查詢或請求閱覽。

請求製給複製本。

請求補充或更正。

請求停止蒐集、處理或利用。

請求刪除。

當事人請求行使查詢或請求閱覽時，若有下列情形之一者，本公司可拒絕當事人行使權利之申請：

妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

妨害公務機關執行法定職務。

妨害本公司或第三人之重大利益。

當事人權利行使之程序

以個資專人為當事人權利行使之負責窗口。如當事人申訴或權利行使申請由個資專人以外之人員收受請求時，應於確認當事人請求內容後轉送個資專人。有緊急狀況時，由個資專人應對之。

當事人行使個資法第3條之權利時，應由當事人本人填寫「個人資料權利行使申請書」及出示身份證明文件向本公司提出申請，並不接受委託法定代理人代為申請相關權利行使作業。

當事人權利行使時應檢具之文件

對本公司行使當事人權利時應檢具下列文件

######  當事人本人提出申請者

 個人資料權利行使申請書

當事人須出示其身分證、健保卡、護照、駕照、居留證或其他足資證明身分之證件以供查驗。

當事人查詢資料應檢具真實文件並據實填寫相關資料，如有虛偽不實者，本公司得拒絕其查詢。

當事人權利行使之回覆

個資專人經審核確認當事人或其法定代理人符合上述資格規定之要件後，應就本公司所保存之現有個人資料進行查詢，並以書面將當事人權利行使之結果回覆當事人，並通知個資管理代表進行結案。

處理期間

本公司受理當事人行使查詢、閱覽、製給複製本之申請後，應於十五日內處理；必要時得延長十五日，並應將其原因以書面通知客戶；如駁回當事人之申請時並附駁回之原因。

本公司受理當事人行使更正補充、刪除、停止處理利用申請後，應於受理日起三十日內回覆結果，必要時，得予延長，延長之期間不得逾三十日，並應將其原因以書面通知請求人；如駁回當事人之申請時並附駁回之原因。

成本費用

對於查詢、閱覽、製給複製本個人資料之申請，本公司得酌收成本費用。相關收費標準如本公司未有訂定者，將參照行政院主計總處提供政府資訊收費標準計算之。

個人資料權利行使申請書，詳見**附件五**。

# 個人資料之風險評估及管理機制

## 個人資料盤點作業程序

### 檢視個人資料檔案

使用個人資料盤點表(如附件六)檢視公司內保有之個人資料檔案，確認個人資料檔案名稱、保有依據、特定目的及資料類別（如表一）。

| **項目** | **說明** |
| --- | --- |
| 檔案名稱 | 文件/檔案的名稱，若為電子檔不用輸入副檔名。例如：本公司會員資料資料庫、會員帳號申請單… |
| 蒐集處理合法情形 | 蒐集、處理個人資料的合法要件: (詳見個資法第 19 條)例如: 與當事人有契約關係、經當事人同意、資料取得一般可取得來源…. 等 |
| 特定目的 | 保有個資檔案之特定目的（可複選）例如：○九○ 消費者、客戶管理與服務，○六七 信用卡、現金卡、轉帳卡或電子票證業務 |
| 資料類別 | 說明個資檔案之項目，分別符合哪些個人資料類別與其細項。例如：Ｃ○○一辨識個人者、Ｃ○○二辨識財務者… |

### 個人資料分類分級

本公司之個人資料依照其屬性、種類、數量、格式及保存方式進行分類分級

個資屬性

一般個資

依據個資法第二條所規定:

指個資檔案含有：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、社會活動及其他得以直接或間接方式識別該個人之資料。

特種個資

###### 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。

###### 此類個資為特種個資，本公司僅在法律明文規定始得蒐集，且蒐集時必須依據個資法規定實施適當安全維護措施：

來源分類

依據本公司之個人資料特性，將本公司之個人資料來源種類區分為

客戶或消費者個資

本公司因執行業務而蒐集外部客戶或消費者之個人資料，例如辦理研討活動、教育訓練而蒐集之客戶或消費者資料(包括非本公司之其他機關公務人員等)。

廠商個資

因與本公司有業務(採購、承包….)往來或承接本公司委外業務而交付之廠商員工或個人之聯絡資訊，此類個資可能為本公司直接向當事人蒐集或廠商間接交付之各類資料，包括個人聯絡資訊、個人財務資訊等等。

員工個資

包括本公司人事部門依法蒐集之正式員工、約聘僱人員等之人員資訊，其中包含各部門不同方式聘用之人事資料包括專案用人、其他計畫等。

其他個資

無法歸類於前三項個人資料之種類。

數量分級

各部門應評估有多少個資數量，100筆與10,000筆個資出現問題對於組織的衝擊會有不同。各部門依據部門的作業特性，可自行對於數量及進行定義以符合個部門的真實狀況。

大量個資：個人資料數量 10,001筆以上。

中量個資：個人資料數量介於 501筆-10,000筆。

小量個資：個人資料數量 500筆以下。

衍生財務危請依據各部門之作業特性，將個人資料之數量自行逕行分級。

資料格式

本公司之個人資料可歸類為以下格式，但注意部分個人資料於處理過程中包含多種個資格式。

紙本：包括一般書表、單據、手寫稿…等。

電子文件/檔案：

###### 電子文件格式: 包括網頁及Email等、PDF 檔等被視為電子文書之書面。

###### 檔案格式：包括各種電子檔格式、備份檔案或暫存檔、郵件附件等，與電子書面格式之不同為此類檔案主要利用方式為檔案，通常用於傳遞或保存。

資料庫格式：各式線上平台系統，存放於資料庫主機內之資料。
(資料庫的備份檔案屬於檔案格式)。

保存方式

依據個人資料的存放及保存方式，本公司個人資料之保存方式可分為：

|  |  |  |  |
| --- | --- | --- | --- |
| **保存方式** | **書面/紙本** | **電子文件/檔案****(郵件、公文、Word、Excel)** | **資料庫** |
| 高安全保存(1)\* | 1.上鎖且保存期間一定有專人管理 | 1.僅有部門管理者可存取或 2.放置檔案伺服器或3.檔案有加密技術保護 | 1.限制連結 或2.僅有系統管理者可存取 |
| 中安全保存(3) | 1.具基本防護/遮蔽 或 2.集中存放 或 3.專人管理 | 1.使用者皆有獨立帳號密碼 或2.個人電腦已有存取控制 或3.檔案有密碼保護 | 1.未限制連結 或2.獨立帳號密碼 且已區分權限 |
| 低安全保存(5) | 1.未有任何管制措施 | 1未有任何管制措施 或2.共用帳號 | 1.未有任何存取措施 或2.共用帳號 |

\*註: 括弧中的數字 (1,3,5) 是用在風險評估時之量化分數使用

## 風險評估作業

### 由個資保管人 (業務承辦人)於個資盤點作業後進行風險評估作業。

風險評估作業，依據本章第一點之分類方式進行對於個人資料檔案之風險評估作業。

依據本公司之作業特性將蒐集個人資料範圍(欄位)進行衝擊性評估。

衝擊性評估表：

|  |  |
| --- | --- |
| 衝擊性 | 評估標準 |
| 低(1)\* | 1. 小量個人資料(500 筆以下)
2. 兩種(含)以內個人資料欄位組合(如：姓名及聯絡電話)且不為高風險資料(如：身分證統一編號、銀行帳號等高風險資料)
3. 從公開資訊取得
4. 資料若遭洩露不會對當事人造成衝擊
 |
| 中(3) | 1. 中量個人資料(501~10,000 筆之間)
2. 三種以上個人資料欄位組合 (如：姓名、聯絡電話、地址)
3. 資料若遭洩露可能會對當事人造成衝擊
 |
| 高(5) | 1. 大量個人資料數量 10,001筆以上
2. 詳細個人資料 (如人事資料、學籍資料等等)
3. 高風險個人資料(如:身分證統一編號、護照號碼、居留證號、銀行帳號、敏感性資料、宗教信仰等)
4. 特種個人資料(病歷、醫療、基因、性生活、健康檢查、犯罪前科)
5. 若遭洩露將對當事人造成身心為害、社會地位受損或衍生財務危機，對當事人造成嚴重衝擊
6. 資料若遭外洩，將嚴重影響公司信譽或業務
 |

\*註: 括弧中的數字 (1,3,5) 是用在風險評估時之量化分數使用

風險分級表

|  |  |  |  |
| --- | --- | --- | --- |
| 衝擊性保存方式 | 低(1) | 中(3) | 高(5) |
| 高安全保存(1) | 低風險(1) | 低風險(3) | 中風險(5) |
| 中安全保存(3) | 低風險(3) | 中風險(9) | 高風險(15) |
| 低安全保存(5) | 中風險(5) | 高風險(15) | 高風險(25) |

### 風險評估作業評估結果為高風險者，應由風險評估執行者(提出風險處理計畫/辦法，風險評估結果為中度風險者，視可改善的方式提出改善建議。低風險者，可以免為進行改善或風險處理計畫。

## 風險管理作業

由前段風險評估作業所評定之個人資料風險，應包括以下作業：

風險評估作業執行

評估作業：由各業務承辦人(個資保管人)進行相關風險評估作業，若評估結果為高風險者，應就該風險項目提出風險處理計畫。

彙整作業：由各部門個資專人彙整各業務承辦人員(個資保管人)盤點出之相關風險評估及風險處理計畫。

核定作業：由各部門個資專人進行計畫之審查後向個資管理代表報告並核定。

風險改善及處理

各部門風險評估作業評估結果為高風險者，應由各部門業務承辦人(個資保管人)提出風險處理計畫/辦法，由各部門個資專人進行相關計畫/辦法之彙整協助，並由部門權責主管進行核准該風險處理計畫，以利將該資產之風險有效控制至低或中度風險。

風險評估結果為中度風險者，可由各部門業務承辦人(個資保管人)視可改善的方式提出改善建議，並由個資專人協助評估。

低風險者，可以免為進行改善或風險處理計畫。

個人資料保護之內部稽核，應審查相關風險處理結果的有效性，以確保所有風險均被有效控制。

風險可接受等級：本公司之風險可接受等級為中風險。

風險處理計畫，其中應包括風險處理計畫說明，執行人員，預計完成日期及所需資源，處理後的風險預估值，所有高風險值應控制到中或低風險。

風險改善管控作業，應由部門主管核准相關計畫後，由業務承辦人(個資保管人)進行後續控管作業，並由各部門個資專人協助，以確保所有改善及風險處理計畫均已依原計畫有效完成控制個人資料之風險。

整體風險評估結果與風險處理計畫應於風險評估作業完成後，由各部門個資專人向個資管理代表進行報告。

風險管理表單：風險評估處理計畫(如**附件七**)。

# 事故之預防、通報及應變機制

個資事件發生時， 由個資專人填製**附件十三**、個資事件通報單，依據本章個人資料事故處理流程進行應變處理；

事件處理完畢後呈報權責主管及個資管理代表。

## 個人資料事件處理流程

### 疑似期：查證引起個人資料事件之原因並做成相關報告。

進行事件的調查，確認事件的真實性及可能的衝擊，並排除誤判或誤報的情形。

由該業務承辦部門協同部門個資專人查證引起個人資料事件之原因並做成相關報告，呈報權責主管並通知個資管理代表。

### 處理黃金期

本公司各業務部門協同個資專人分析案由，提交權責主管，並通知個資管理代表。

由本公司各業務部門協同個資專人、稽核專人及本公司法律諮詢顧問討論可能之法律責任。

各業務部門協同個資專人就事故之範圍，擬定事故通知之當事人及相關部門。

如事故涉及一個部門以上時，應由本公司個人資料保護聯絡窗口為單一協調窗口，進行後續之事故處理及通知當事人。

由個人資料保護聯絡窗口召集本公司相關部門及本公司法律諮詢顧問與當事人召開事故協調會避免事件擴大。

### 事故擴大期

由本公司業務部門協同個人資料保護聯絡窗口及法律諮詢顧問組成事件說明小組向外說明，其對外發言部分得由個資管理代表指定，並應同時要求本公司所有同仁不得自行針對此事件發言。

由本公司業務部門協同個人資料保護聯絡窗口及法律諮詢顧問共同擬定訴訟策略。

### 司法訴訟

由本公司業務部門協同個人資料保護聯絡窗口及法律諮詢顧問共同擬定訴訟策略。

由本公司業務部門協同個人資料保護聯絡窗口及法律諮詢顧問就訴訟策略進行訴訟。

由本公司業務部門協同個人資料保護聯絡窗口及法律諮詢顧問尋求事故和解之可能性。

## 個人資料事件通報管理

本公司個人資料事故通報流程：

### 內部通報流程

本公司所有人員發現疑似資安或個資事故現象，應立即通知本公司各業務部門或部門個資專人。

### 外部通報流程

客戶或消費者如果透過本公司申訴管道通報疑似資安或個資事故時。或由其他本公司以外部門通知本公司時，應立即通知本公司各業務承辦部門或個資專人。

### 事件之紀錄與處理

各業務部門或個資專人接收到相關通報，應記錄事件通報內容，並依本章之事件處理程序進行處理。

## 個人資料之事件懲處管理

各業務部門或個資專人於查明相關人員疏失之責任歸屬後，應視情節之輕重呈請權責主管或個資管理代表為適當之後續處理。

# 資料安全管理及人員管理

本公司之資料安全管理措施要求共分為四大類安全措施，個資專人應進行本公司內之資料安全管理措施之推行，並視需求回報權責主管或個資管理代表執行狀況及資源需求。

## 資料安全防護措施

蒐集作業安全防護措施

紙本蒐集方式：以紙本方式進行個人資料之蒐集，應進行以下之防護措施：

紙本應進行紀錄管制，視紀錄之重要性，透過編號及安全等級標示(密級、內部使用、公開等，公開等級可以不標示)，含有個人資料之紀錄應至少標示為內部使用。

蒐集之紙本應進行紀錄管制，除進行對於該資料歸屬之卷宗進行機密等級標示，並應進行實體存取之防護(例如鎖於櫃子內) 。

須依據法規盤點及個資盤點結果之保存年限要求進行保存。

媒體蒐集方式：透過媒體(CD/DVD/TAPE等)接收個人資料檔案需進行以下防護：

如媒體數量超過三項，或為經常性(如按月蒐集)蒐集者，應建立清冊進行數量管制。

媒體應明確標示媒體內儲存之內容。

媒體應進行實體存取之防護。

媒體資料輸入資訊系統後，應視其需求進行保存，如不須保存該媒體，應進行媒體報廢作業進行銷毀。

網站蒐集方式：透過本公司網站進行個人資料之蒐集時，應進行以下防護措施：

確保輸入之網頁具有 SSL (Secured Socket Layer)等安全措施(或其他對等之安全措施)，確保該蒐集作業不在傳輸過程遭未授權存取或擷取。

網頁所產出之資料檔案應注意其安全防護，該資料檔案不應置放公共可存取之目錄。

網頁程式或網站系統所保存之暫存檔(Server Log, Server Cache檔)應定期刪除或確認存放於伺服器內避免遭受未授權之存取，並確認暫存檔中可能留存的個人資料之保護狀態。

本公司蒐集個資紀錄，宜採電子型式由當事人自行填寫，並限制僅蒐集與特定目的相關、不可或缺的個資欄位。

處理作業安全管理措施

資料加密

對於重要的資料、高敏感資料(例如特種個資)，或洩漏、誤用可能對當事人有高衝擊性的資料(例如金融帳號等)，由各部門於風險評估過程中進行識別及評估，如需使用加密(Encryption)技術降低風險者，應注意以下方式：

加密使用金鑰須妥善保存，不應將金鑰存放於系統程式、資料庫中。

加密算法，應使用安全的算法及金鑰長度，目前應使用 AES128 或其他相同強度以上的加密算法及強度。

去識別化作業

本公司因蒐集的個人資料，如無須識別當事人者應以去識別化方式為之，藉由代碼替換、刪除或隱藏部份個資欄位，使該個資紀錄無法直接識別當事人。

處理設備之實體安全

請參考本文件**壹拾、設備安全管理**。

處理設備之邏輯安全及網路安全

請參考本文件**壹拾、設備安全管理**。

資料儲存設備之安全

請參考本文件**壹拾、設備安全管理**。

資料備份，個人資料有備份需求者，其備份資料應與原資料有相同 全等級的保護。

資料傳輸安全，個人資料需進行網路傳輸時應做到

對原有資料進行加密後傳輸，或

透過安全通道協定，例如 SSL, TLS, 或其他點對點安全傳輸機制，安全傳輸的協議(例如 SFTP 等)，嚴禁使用不安全的傳輸方式進行資料傳輸(例如為TLS 1.0, SSL 3.0, FTP 等等) 。

資料正確性檢查

應用系統或網站系統，應於蒐集個人資料後，進行對於資料正確性的檢查，例如身分證字號檢核碼、電話號碼格式、 Email 格式等。

重要個人資料之輸入作業，應於輸入作業完成後，進行資料正確性之複核作業。

資料於傳輸或接受後，應進行資料正確性之檢查，確保傳輸/接受前後之資料正確性。

刪除作業(依據當事人權利要求)

個人資料保護法所規範之刪除，應使個人資料於個人資料檔案中消失，因此，資料的刪除作業應確保下述事項：

該資料於個人資料檔案中消失，包括備份之資料。

以去識別化方式進行刪除時，應注意該資料不應於去識別後得以其他方式重新組建其具識別性之欄位。

刪除作業應確保位於暫存檔案、原始紙本、原始資料檔案或媒體之資料也同時被刪除。

資料利用作業安全防護措施

資料利用之安全防護控管

資料之利用除須依本文件的利用管理程序進行申請外，並應於核准該利用時，檢核其利用過程之安全性。

資料傳輸至其他部門之控管

紙本傳輸

###### 如必須應指派人員親自交付。

###### 透過公文傳遞者，應視情形進行密件標示處理。

###### 需透過郵遞業者傳遞紙本時，應以掛號方式寄出，並應進行該紙本資料密封作業。

電子傳輸

###### 應避免以沒有安全防護之電子傳輸方式進行個人資料之傳輸。

###### 以電子傳輸個人資料，至少應以 Winzip 等壓縮軟體進行通行碼(Password)保護，並以分開的傳遞方式遞送該密碼。

###### 視需求得以加密(Encryption)方式進行資料加密，以確保檔案之機密性。

###### 傳輸前，應確認接收端之收件人、位置、主機等資訊，確保不在傳輸過程中遭攔截或竊取。

###### 大量資料電子傳輸或經常性資料電子傳輸應進行申請，由權責主管或個資管理代表確認其安全性後始得進行。

## 資料存取安全措施

執行個人資料處理之資訊系統或資料庫，其存取控制應包括：

帳號唯一性原則

所有帳號應為唯一性，如非必須，不得多人共用帳號。

帳號共用應事先經過權責主管及資訊系統負責人之同意，並於適當安全配套(如增加其可歸責性措施)後使得進行。

嚴禁帳號之借用，以避免破壞帳號使用之可歸責性。

### 帳號核發、變更及刪除方式

帳號之核發，應經過申請核准，並紀錄其使用人員及使用期間。

帳號之啟用及通行碼(Password)發放，應有安全防護，以避免遭他人未授權使用。

帳號之變更應經過事先之申請審核，並留存相關紀錄。

帳號於人員離職或變更職務後應進行刪除或停用，如需保留一定的期限，應填寫申請單，經權責主管之核准。

帳號通行碼(Password)原則

處理個人資料之資訊系統其通行碼原則應，其通行碼強度應至少為八碼，內含英文、數字、大小寫等複雜度要求。

軌跡資料保存

申請及變更資料

所有個人資料蒐集、處理、利用之申請作業與變更作業應留存適當之軌跡資料。

帳號之申請作業紀錄(電子紀錄及紙本紀錄)應至少保留五年。

使用者(當事人)申請之存取帳號作業紀錄，如無其他法律規定保留期限，應至少保留五年。

存取紀錄

個人資料之存取紀錄，應留存其存取紀錄，重要個資檔案或個人資料主檔資料庫之存取紀錄應至少保留五年。

定期審查存取權限

有關個人資料之資訊系統或資料庫系統存取權限，應至少每年進行一次存取權限之審查。

## 資料存放安全措施

紙本資料

紙本資料應進行實體存取之安全管控，大量紙本保存時應注意該紙本事後檢索、取回之可能性及作業方式，以因應當事人進行刪除之請求。

紙本之存放應注意防潮及防火，避免意外毀損紙本個資。

紙本存放之倉庫，應注意其安全性，如與其他物品共置於一室內，應透過監視防護措施，或其他安全管制制度(例如人員陪同)進行其存取控制防護。

電子資料(存放於電腦或伺服器)

存放於個人電腦者

電子(檔案、資料庫等)型態之個資存放於個人電腦，應注意該電腦至少應裝設防毒軟體並定期更新病毒碼，嚴禁使用。

電子型態之個人資料存放於個人電腦，應確保僅存放最少之需求資料，以避免過多資料存放之風險。

經常性存放個資於個人電腦者，應確保該電腦有足夠安全防護。

個人資料存放於個人電腦者，如必要時應進行資料之加密，以降低資料遭竊取、遺失之風險。

存放於電腦伺服器者

檔案伺服器等應嚴禁以未有存取控制之方式進行檔案共享。

檔案伺服器之存取權限應視需求開放，並應定期檢視其存取權限之設定。

檔案伺服器之管理者權限應控制其必要數量，避免過多的管理者權限可存取非業務相關之資料檔案。

存放於檔案伺服器中之檔案，應視需求定期進行檢視，確保其存放之安全防護需求。

視需求高重要或大量個人資料存放之檔案應進行加密作業，以避免個資洩漏、遺失之風險。

檔案伺服器應留存相關存取紀錄，並由管理人員定期檢視是否有異常之存取行為。

資料儲存媒體

#### 可移除式媒體(含行動硬碟、USB、CD、DVD等媒體)未經核准不應使用可移除式媒體進行個人資料之複製或備份。

## 資料備份安全措施

備份作業之規劃

訂定備份政策

應訂定備份政策進行個人資料檔案之備份作業。

訂定備份計畫或清單

備份管理人員或系統管理人員應依據備份政策進行該資訊系統或檔案之備份作業，並產出備份計畫或清單，透過人工或工具進行備份並留存紀錄。

評估及訂定備份的安全防護需求

對於備份後的備份檔案應視其存放之媒體種類、存放之位置、系統、既有之安全防護評估並擬定備份檔案之安全防護需求，並依據該需求進行防護措施的實施，並將結果紀錄於備份計畫或清單表格內。

評估及訂定備份的測試需求

針對備份計畫或清單內之備份結果，應評估該備份資料之重要性及其還原需求之頻率、可能性進行評估後產出備份測試之需求。

備份作業執行及紀錄

於備份計畫或清冊內紀錄下述事項：

記錄備份之執行狀況。

記錄備份之儲存位置及保護措施。

記錄備份之目的、使用方式。

### 備份作業之監督及測試作業

定期審查備份作業之正確性。

定期執行備份資料之盤點作業。

盤點備份資料須注意備份檔案可能存放在以下媒體：

TAPE

DVD/CD/DDS

存放於媒體或虛擬主機(Virtualized Server) 上(Ghost檔、Image 檔案或 Snapshot 檔案)

伺服器、儲存設備內之檔案

###### 檔案伺服器內

###### 網路儲存設備內(例如 NAS等)

###### 遠端主機、遠端儲存設備、網路儲存設備等

###### 可移除式媒體上

可移除式硬碟

USB 儲存設備

###### 資料庫主機之備份、備援主機、備份資料庫主機等

備份媒體之測試

依據測試需求擬定測試計畫。

於測試執行後將測試結果記錄於備份計畫或清冊內。

## 人員聘僱管理

### 人員任用

正式職員、約聘僱人員及其他計畫或臨時人員依照本公司人事管理相關之規定辦理。

本公司新進人員於報到時，應於人事契約中或單獨簽定保密切結書，確保對於業務接觸之個人資料負保密的義務。

本公司資訊業務委外服務之廠商或人員，應於簽訂契約時同時簽署保密切結書(或於合約中包含個人資料保護之相關條款)，遵守本公司個人資料保護管理規定。

帳號及電子郵件之使用申請，均應確實依人員之任離職及工作執掌變動情形填列帳號申請單，以利進行帳號管制。

本公司同仁離職時，須依照人事單位規定填寫離職單確保於離職後仍對在職期間接觸的個人資料負保密義務，始完成離職程序。

應用系統使用者如因職務異動而成為非授權使用者時，相關部門應主動通知系統管理人員及各業管部門管理人，同步異動該使用者帳號及操作權限。

### 人員職務異動或離職

本公司同仁離職或職務異動時，應進行資產之移交，以防止人為舞弊或個人資料及資訊資產損失之風險。

本公司同仁離職或職務異動時，應依照規定變更或註銷其相關系統之使用權限。

## 機密維護責任

### 本公司同仁應遵守「個人資料保護法」等相關規定，以及本公司之個人資料檔案全維護計畫，於辦理與個人資料及資訊安全之相關業務時，因業務所獲知之機密資訊，非經權責主管授權不得對外透露。

### 為確保本公司個人資料及資訊安全，若與往來廠商簽訂合約，應依據**陸、個人資料委外管理程序章節**之規範訂定合適之合約內容；廠商人員應遵守合約及本規定有關個人資料及資訊安全之規範，並簽訂「合約廠商保密切結書」，對於執行業務所獲知之資訊，非經本公司授權同意前不得對外透露。

## 人員資訊作業注意事項

應遵守本公司所有個人資料及資訊安全之相關規定。

所有本公司同仁(含新進職員、約聘雇人員)均應接受個人資料及資訊安全之訓練課程。

不得自行安裝非法軟體於個人電腦。

不得以任何手段蓄意干擾或妨害網路系統的正常運作。

禁止利用本公司網路資源從事個人網站營利及不法情事。

不得隨意開啟來路不明的電子郵件，以免啟動惡意執行檔或連結。

帳號密碼必須定期更換，且不得洩露予他人。

禁止冒用他人的帳號及密碼登入電腦操作系統。

未經授權人員不得進入電腦機房。

所有個人電腦含筆記型電腦在經過15分鐘的閒置後，必須啟動設有密碼的螢幕保護程式。

屬於機密等級需控管之資料，離開座位時勿停留在螢幕畫面，敏感及機密文件不得留置於桌面。

下班時應關閉個人電腦與螢幕電源。

禁止使用違反智慧財產權相關的資訊資產。

# 設備安全管理

個資法要求對於個人資料處理設備進行安全的管控，本公司對於設備安全管理之程序分為

## 個資處理設備清查

進行對於本公司內部個資處理設備之清查作業，透過清查進行對於設備的識別，確保所有與個人資料蒐集、處理、利用作業相關之設備均於此過程中被清查出，以便後續進一步的評估設備所需要的安全要求。

### 個人資料輸入處理設備

辦公輸入設備：掃描器、傳真機、影印機等用來處理紙本資料個資蒐集設備。

個人資料輸入管道：包括網站設備等可能用來接收或處理蒐集個人資料之設備。

個人資料處理設備

個人電腦設備：包括人員使用之個人電腦設備、筆記型電腦、手持式電腦設備等資料處理設備。

檔案伺服器：儲存檔案的公共檔案主機，包括各類、各種技術形式的檔案集中儲存設備。

資料庫主機設備：主要以資料庫形式(包括各種不同資料庫，例如 SQL Server, My SQL, Access Database, LDAP …)存放個人資料的設備。

通訊設備：例如傳真機，答錄機，影印機等通訊設備，因目前科技進步，該等設備內均有設置儲存裝置(例如硬碟機)，以加速或增加該設備的功能，因而可能因為當事人傳真進本公司或本公司人員影印相關含個人資料之紙本而在該等設備中留存部分個人資料(此類設備維護廠商通常可以檢視或存取該儲存裝置)。

其他資料處理設備：例如各式側錄主機(例如 Email 側錄設備，社交通訊軟體側錄設備，網路訊息側錄設備)，各類Log 紀錄蒐集及分析設備。

資料儲存設備

備份空間、伺服器(包括異機備份、SAN 或NAS 網路儲存設備)。

備份媒體、磁帶、光碟、DDS等之儲存設備。

## 設備安全需求

對於處理個人資料設備於清查後應進行該設備安全需求控管作業，包括以下：

設備實體安全防護措施

評估設備需要適當的實體安全控管，例如

應有實體存取預防措施：例如上鎖、加上密碼控管、專人看管、或其他實體保護。

如設備數量較多，應進行數量的盤點及控管，確保該等設備無遭竊之可能。

設備邏輯及網路安全防護措施

如果設備可以接上網路、通訊網路等邏輯(非實體)通路時，應注意對於此類網路安全的需求

設備之網路安全措施

應有適當的網路安全措施，例如進行適度的網路區隔，進行網路位址轉換技術(例如使用NAT Network Address Translation) 以確保網路位址(IP) 位置不被外部人員所知悉，安裝防火牆設備或設定連線端條件(固定IP、 回撥、特殊路由等)。

設備安全管理措施

建置防火牆、電子郵件過濾機制或其他入侵偵測設備等防止外部網路入侵對策，並定期更新。

系統存有個人資料者，應設定異常存取資料行為之監控及定期演練因應機制。

確認蒐集、處理或利用個人資料的電腦、相關設備或系統具備必要之安全性防護，採取適當之安全機制，定期檢測並因應系統漏洞所造成之威脅。

與網路相聯的資訊系統存有個人資料者，應隨時更新並執行防毒軟體，及定期執行惡意程式檢測。

處理個人資料之資訊系統有變更時，應確保其安全性未降低。

定期檢視處理個人資料之資訊系統，檢查其使用狀況及存取個人資料之情形。

資料傳輸安全防護措施

此類設備在傳輸資料時，應進行額外的資料保護，例如傳輸加密、安全通道、VPN 等強化傳輸安全之防護措施。

資料安全防護措施

如果設備具備存放或短暫存放資料的能力，應針對此類設備進行資料安全的防護包括

資料機密性的保護需求：資料應進行機密性的保護，例如加密機制、設置存取控制、通行碼管制、進行資料遮罩等。

該設備應於送修、維修前移除資料或以其他方式控制不被維護廠商未授權存取。

該設備應進行資料完整性的保護，例如避免震動、電流不穩、資料傳輸後複核等保護。

資料可用性的保護：規劃該設備進行備份，不斷電保護及其他確保資料可用性之防護。

處理個人資料的資訊系統進行測試時，應避免使用真實個人資料；使用真實個人資料者，應訂定使用規範。

評估使用情境，採行個人資料之隱碼機制，就個人資料之呈現予以適當且一致性之遮蔽。

設備存取權限之管制措施

如果設備可以讓多人進行存取，應進行存取權限的控管保護，包括

帳號申請作業需求，應具備帳號申請作業，確保開放該設備存取之過程經過相關人員核准。

帳號存取權限安全措施：例如帳號長度控管，通行碼更換頻率，通行碼複雜度及通行碼的交付安全保護。

帳號審查作業：應進行定期的帳號權限審查，以確保該設備之存取權限開放均為正確。

其他防止未授權存取的安全保護：例如進行一次性密碼(OTP, One Time Password), 雙因認證等強化存取控制的作法，螢幕保護控制、會談時間過期(Session Time Out)等對於存取控管的安全防護。

# 認知宣導及教育訓練

## 訓練需求評估

執行人員

本公司之個人資料安全教育訓練由教育訓練小組負責規劃及執行。

執行時間

於每年一月產出本年度之教育訓練計畫，並由個資管理代表或授權之權責主管審核後，由教育訓練小組執行。

評估及課程需求內容

評估內容依參考(須包含)：

法規變化

主管機關提出之教育訓練需求

人員個資保護知識需求

配合資安教育訓練

本公司個資保護管理政策及安全維護計畫內容

針對人員的特殊教育訓練內容

針對個單位個資專人或權責主管，除一般人員的認知宣導課程外，每年至少一次，應進行個資管理人員訓練，其訓練內容包含：

個資法法律訓練

目的事業主管機關管理辦法訓練

當事人權利行使作業訓練

個資風險管控管理訓練

針對各部門業務承辦人(個資保管人)，每年應進行至少一次，個資保管人員訓練課程，內容包含：

個人資料法律訓練

個人資料盤點訓練或工具使用訓練

個資保護風險評估管理訓練

針對內部稽核人員，每年應進行至少一次，個資保護內稽人員訓練課程，內容包含：

個資法與主管機關管理辦法的稽核要求

本公司個資保護管理計畫

內部稽核技巧訓練

內部稽核報告書

稽核後續管理(矯正預防措施)

## 訓練計畫

教育訓練小組於每年一月產出本年度之教育訓練計畫，並由本公司個資管理代表審核後，由教育訓練小組執行。

## 訓練執行

由教育訓練小組委由本公司內部人員或聘請外部講師進行訓練；或由各部門及各部門透過教育訓練平台進行相關課程之影像檔播放。針對各項教育訓練，於結束後可利用評量/問卷等方式進行有效性評估。

## 訓練結果維持

教育訓練成果紀錄應予以留存，並呈報個資管理代表。

## 成效評估與計畫修正

於每年之成效報告後，應提出隔年之教育訓練計畫之修正，如有重大差異或成效缺失，應提出矯正預防計畫，確保教育訓練之成效管理。

# 資料安全稽核機制

## 稽核人員

本公司之個人資料安全稽核由稽核小組及指派之稽核人員進行，稽核人員指派的原則，應以具備稽核知識與能力，並與受稽核業務或人員保持一定的獨立性為原則。

## 稽核管理

本公司之個人資料保護管理內部稽核工作之執行者不僅限於本公司稽核人員，亦可委由外部具備專業資格之人士進行，但不論由內部或外部人士執行，稽核人員必須具備獨立性及客觀性，內部稽核人員不能稽核本身之工作。

稽核工作必須對稽核過程所查核事項的事實加以紀錄，以顯示其稽核軌跡作為稽核發現之佐證。

稽核所發現之缺失及觀察事項與建議，應由稽核人員及被稽核部門就是否屬實取得一致之見解，被稽核部門應對稽核所見加以檢討並尋求改善，稽核結果及改善行動執行情況應交付本公司個資管理代表或其指派之人員。

### 稽核準則包含以下規定：

個人資料保護法。

個人資料保護法施行細則。

主管機關對於個資保護管理相關作業管理辦法。

本公司個人資料保護政策及個人資料安全維護計畫。

本公司個人資料保護管理規定及各部門作業內容。

## 稽核計畫

實施個人資料保護內部稽核前，內稽小組或稽核人員擬定個人資料安全稽核計畫以及個人資料安全稽核查檢表後，得經由稽核小組審核後執行。

稽核人員得於預定執行時間一個月前就該次稽核編定其執行計畫，稽核計畫之制定須考慮過去稽核之結果決定稽核範圍及查核重點。稽核人員應於評估本公司作業週期及風險後，擬定包含稽核目的、稽核項目、稽核對象、實施期程、稽核方法、作業程序、稽核重點及稽核結果等之稽核計畫，依照所排訂之稽核項目，訂定作業程序及稽核重點，稽核時並得依情況適時調整。

稽核計畫得經個資管理代表審議後核定實施，修正時，亦同。

稽核人員應與受稽部門主管事前溝通，確定稽核時間及相關協調工作。並於稽核7日前，通知受稽核部門。

## 稽核範圍

個人資料保護告知事項及同意內容 (個資法第 8 條及第9 條要求)。

個人資料盤點作業與個人資料範圍界定作業(施行細則第12條第 2 項第 2 款規定)。

個資法規盤點作業(本文件第肆章要求)。

風險評估與風險管理作業(施行細則第12條第 2 項第 3 款規定)。

個人資料事故之預防、通報及應變作業。(施行細則第12條第 2 項第 4 款規定)。

個人資料蒐集、處理、利用行為之檢查(施行細則第12條第 2 項第 5 款要求)。

資料安全維護作業檢查(施行細則第12條第 2 項第 6 款規定)。

認知宣導及教育訓練作業檢查(施行細則第12條第 2 項第 7 款規定)。

設備安全維護 (施行細則第12條第 2 項第 8 款規定)。

個人資料保護持續改善作業(施行細則第12條第 2 項第 11 款規定)。

使用紀錄、軌跡資料及證據保存作業檢查(施行細則第12條第 2 項第 10 款規定)。

當事人行使權利所執行之各項檢查。(個資法第 3 條及第10、11、13 條要求)。

## 稽核頻率

本公司個人資料保護管理每年執行一次定期稽核，對於特殊事項之稽核，本公司管理代表得指派人員進行特別追蹤稽核。

## 稽核方法

稽核採抽樣方式進行，對於特別查核項目之抽樣數可由稽核人員指定。

## 稽核紀錄與報告

稽核工作必須保留工作底稿(如**附件九**)，工作底稿可為電子檔或書面手寫，但須清楚顯示每一查核項目之查核準則、訪談對象、所檢視紀錄及所進行之抽樣及該項查核之結果。

對於不符合事項必須填具稽核報告單，提供受稽部門進行改善作業。

稽核人員須於稽核結束兩週內提交稽核報告，報告須包括各項建議、觀察事項及不符合事項之彙整及統計、對於整體個人資料保護管理之有效性及適切性之評估以及就稽核過程之有效性的自我檢討與評估。

稽核人員依據稽核工作底稿及審定「內部稽核觀察、建議及回覆紀錄表」 撰寫「稽核報告」，稽核報告經個資管理代表覆核、審查。

## 稽核改善與追蹤

### 稽核後續須進行改善與及改善之追蹤，其方式如下：

受稽部門填寫矯正措施單 (如**附件十一**)

稽核人員依受稽核部門所提出之預定完成改善期限進行追蹤查核。

稽核人員依據稽核追蹤工作底稿撰寫「追蹤報告」。

受稽核部門之改善事項未於改善期限完成或未執行改善者，稽核人員應於「追蹤報告」中明確記載。

「追蹤報告」應經受稽核部門會簽後，呈送個資管理代表核閱。

改善事項未於改善期限完成或未執行改善追蹤事項者，內部稽核小組應將相關書面資料，通知個資管理小組，列入部門年度考核之參考，並列入下次稽核重點。

稽核時所發現之不符合事項，應於年度稽核報告中據實揭露，並檢附工作底稿及相關資料，作成稽核報告，定期追蹤至改善為止。稽核報告、工作底稿及相關資料，應至少保存五年。

# 個人資料安全維護之整體持續改善

## 程序目的

本公司個人資料保護須依循管理系統之PDCA (Plan, Do, Check, Act)循環，除本公司於計畫階段進行訂定個資保護政策、個資保護安全維護計畫及要求人員遵循政策及本規定外，本程序將建立持續改善之方式以確保本公司對於個資管理的有效性。

## 檢查

本公司透過稽核機制及通報機制進行相關個資遵循的檢查作業包括：

### 例行性的個人資料保護稽核作業。

### 設置個資專人，針對個人資料保護進行例行性的檢查作業。

### 個資保護執行作業報告。

本公司於年度召開由本公司相關作業執行人員進行個資保護各項相關作業之成果報告，並統計相關資訊後提供給本公司進行彙整，以確保所有之個人資料檔案安全維護計畫執行結果均符合本公司之需求。項目得包括：

教育訓練作業報告

預計後續個人資料保護認知及教育訓練年度規劃。

本年度個人資料保護教育訓練之成效。

資訊保護作業報告

該年度的個人資料相關事故統計及處理情形。

其他個人資料保護相關議題。

內部稽核作業報告

該年度內部稽核報告。

矯正預防措施。

當事人權利管理作業報告。

當事人權利申請狀況及處理結果。

風險管理作業報告。

個人資料風險評估結果。

風險管理結果報告。

個人資料保護管理作業情形進行報告。

## 持續改善

於各項檢查後之發現結果，各業務承辦部門應該針對該發現點提出矯正措施包括：

發現原因，事件發生或異常發生的原因。

矯正計畫：針對原因提出解決方案。

計畫預計完成日期：矯正措施所需之完成時間預估。

計畫執行人員：指派之矯正措施執行人員。

需求資源：完成計畫所需之資源，包括人員、預算或相關資源之需求。

矯正計畫之審查

矯正措施之提出，應由該部門權責主管進行核准後監控執行到完成，後將相關執行結果送交管理代表簽核後結案存查。矯正措施單之格式如**附件十一**。

# 附件一、個人資料保護管理小組組織名單

更新日期: 年 月 日

|  |
| --- |
| **個人資料保護管理小組組織名單** |
| **人員** | **部門** | **職稱** | **姓名** | **聯絡方式** |
| 管理代表 |  |  |  |  |
| 聯絡窗口 |  |  |  |  |
| 聯絡窗口 |  |  |  |  |
| **預防/通報/應變小組** |
| 小組長 |  |  |  |  |
| 組員 |  |  |  |  |
| 組員 |  |  |  |  |
| **教育訓練小組** |
| 小組長 |  |  |  |  |
| 組員 |  |  |  |  |
| 組員 |  |  |  |  |
| **稽核小組** |
| 小組長 |  |  |  |  |
| 稽核人員 |  |  |  |  |
| 稽核人員 |  |  |  |  |
| **各部門個資專人** |
| 個資專人 |  |  |  |  |
| 個資專人 |  |  |  |  |
| 個資專人 |  |  |  |  |
| 個資專人 |  |  |  |  |
|  |  |  |  |  |

# 附件二、個資保護適用法規一覽表

 更新日期: 2023/12/16

|  |  |  |  |
| --- | --- | --- | --- |
| 編號 | 法律規定名稱 | 生效/修訂日期 | 相關連結 |
| 1 | 個人資料保護法 | 112/05/31 | https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021 |
| 2 | 個人資料保護法施行細則 | 105/03/02 | https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050022 |
| 3 | 個人資料保護法之特定目的及個人資料之類別 | 101/10/01 | https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=fl010631 |
| 4 | 數位經濟相關產業個人資料檔案安全維護管理辦法 | 112/10/12 | https://law.moda.gov.tw/LawContent.aspx?id=GL000090 |
| 5 | 第三方支付服務業防制洗錢及打擊資恐辦法 | 112/02/24 | https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=J0080060 |
| 6 | 洗錢防制法 | 112/06/14 | https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=G0380131 |
| 7 | 行政院主計總處提供政府資訊收費標準 | 101/06/08 | https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=T0010009 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 附件三、新個資蒐集前查檢表

|  |
| --- |
|  新個資蒐集前查檢表 |
| 申請人 |  | 申請日期 |  |
| 業務名稱 |  |
| 內容摘要 |  |
| 蒐集類別 |  |
| 特定目的 |  |
| 相關法源依據及法律要求說明(例如：最小保存時間) | 法律名稱： 條文: |
| 蒐集方式說明 |  |
| 蒐集格式 | □ 紙本 □ 電子文件/檔案 □ 資料庫 |
| 預計保存時間 |  |
| 保存方式 | □ 紙本 □ 電子文件/檔案 □ 資料庫 |
| 預計利用方式(期間、地區、方式) |  |
| 蒐集方式 | □ 直接蒐集 □ 間接蒐集 □ 委外蒐集 |
| 如為間接蒐集 | 間接蒐集資料來源:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_來源分類: □合法公開資料庫□公開可取得來源□其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_間接蒐集資料來源合法性檢查:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 第19條蒐集處理合法要件 | □法律明文規定。□契約或類契約關係。□經當事人書面同意。□對當事人權益無侵害。□其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 其他項目檢查 | 內容 | 是否符合 |
| 告知函撰寫 |  |  |
| 委外合約監督條款擬定 |  |  |
| 會簽意見 |
| 個資專人(可提供法律意見同仁或小組) |  |
| **核准紀錄** |
| 申請人 |  | 日期 |  |
| 部門主管核准 |  | 日期 |  |
| 個資專人 |  | 日期 |  |
| 個資管理代表 |  | 日期 |  |

# 附件四、新個資利用前申請書

|  |
| --- |
| 新個資利用前申請書 |
| 申請人 |  | 申請日期 |  |
| 將利用之個資說明 (說明利用的標的及簡述利用之狀況) |  |
| **現有個資蒐集、處理、利用狀況說明** |
| 🞏 直接蒐集資料🞏 間接蒐集資料：取得來源說明 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_告知義務：🞏 已依個資法第8條或第9條進行告知 🞏 依法免告知\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_目前資料保存方式、存放地點:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_目前資料管理部門及管理人員: 🞏 同申請部門🞏\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **個人資料檔案說明** |
| 個人資料檔案名稱 |  |
| 範圍 |  |
| 檢附文件 |  |
| **預計利用方式說明** |
| 利用之方式說明 (方式、對象、地區、期間) 交付方法、安全措施 | 方式:期間:地區：對象: |
| 與原蒐集目的檢查 | 是否與原蒐集作業已告知之利用方式、對象、期間、地區相符或與原蒐集目的相符🞏是 🞏否 🞏保留意見\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 利用是否為法律明文規定 | 🞏是 🞏否 🞏保留意見\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 利用是否於原蒐集之特定目的必要範圍內 | 🞏是 🞏否 🞏保留意見\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 利用方式(傳遞方式)是否合乎適當安全維護之規定 | (例如：原有資料傳遞方式如電子郵件、光碟等之保護措施) |
| **會簽意見** |
| 個資專人(可提供法律意見同仁或小組) |  | 🞏是🞏否🞏不適用 |
| **核准** |
| 申請人 |  | 日期 |  |
| 部門主管核准 |  | 日期 |  |
| 個資專人 |  | 日期 |  |
| 管理代表 |  | 日期 |  |

# 附件五、個人資料權利行使申請書

|  |
| --- |
|  **個人資料權利行使申請書** |
| 申請人 |  | 申請日期 |  |
| 申請事項 |  □查詢 □閱覽 □複製本 □更正 □補充 □停止蒐集 □停止處理 □停止利用 □刪除 |
| 檢附文件 |  |
| 申請事由:本人\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_之需求向 貴公司申請個人資料之 □查詢 □閱覽 □複製本 □更正 □補充 □停止蒐集 □停止處理 □停止利用 □刪除 之作業。擬請 貴公司協助處理作業。 |
| 查詢 | (請填寫需求例如範圍、期間….) |
| 閱覽 | (請填寫需求例如範圍、期間….) |
| 製給複製本 | (請填寫需求例如範圍、期間、需求份數等….) |
| 更正 | (請填寫需求例如範圍、資料欄位….) |
| 補充 | (請填寫需求例如範圍、資料欄位….) |
| 停止蒐集、處理、利用 | (請填寫需求例如範圍、資料欄位….) |
| 刪除 | (請填寫需求例如範圍、資料欄位….) |
| 申請人權益影響說明(申請停止蒐集、處理、利用及刪除者)1. 申請停止蒐集、處理、利用者，因本公司系統因未能處理個人資料，因而造成部分之系統功能無法正常運作，當事人權益將因申請停止前述動作而有影響，其影響之結果申請人同意自行承擔。2. 申請刪除作業者，申請人了解資料一經刪除後無法復原，因為刪除個人資料後造成之申請人於本公司服務之權益損失將自行承擔，並不再提出恢復資料之要求。□申請人詳閱並同意上述權益影響說明: |
| 申請人簽名 |  | 日期 |  年 月 日 |
| **處理結果(由本公司填寫)** |
| 受理部門審查意見 | * 接受(符合本公司申請條件)
* 拒絕(不符合本公司申請條件)
* 酌收資料處理費(查詢/閱覽/製給複製本)： 元
 |
| 受理部門人員 |  | 日 期 |  年 月 日 |
| 受理部門主管 |  | 日 期 |  年 月 日 |
| 個資專人 |  | 日 期 |  年 月 日 |

# 附件六、個人資料盤點表(另提供 Excel 檔)



# 附件七、風險處理計畫(提供 Excel 表)

| 現況說明 | 風險改善措施 | 負責部門 | 預計改善時間與處理方式 | 風險評估彙整表對照 |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

# 附件八、教育訓練成果報告表

|  |
| --- |
| 教育訓練計畫 製表日期 年 月 日 執行教育訓練負責人( ) |
| 教育訓練名稱 |  |
| 教育訓練目的 |  |
| 教育對象 |  |
| 執行教育訓練人(講師) | 總計 名 |
| 使用資料 |  |
| 執行日期 | 場所 |
| 例) 第1次 年 月 日 |  |
|  第2次 年 月 日 |  |
| **教育訓練內容** |
| <反應上次教育訓練內容> |
| <教育訓練內容> |
| 確認教育訓練效果方法 | 例)問卷調查、隨堂測驗 等 |
| 教育訓練負責人  |  年 月 日  |
| 執行教育訓練紀錄 製表日期 年 月 日 製表人( ) |
| <執行教育訓練內容> |
| <應出席學員人數/出席學員人數說明>  |
| <本次教育訓練結果應反映於下次教育訓練事項> |
| 教育訓練結果處理 | □ 不須處理 □ 需要追蹤教育訓練 □其他 |
| 處理內容 |  |
| 教育訓練負責人 審核 |  年 月 日  |
| 個資保護管理代表 核決 |  年 月 日  |

# 附件九、稽核查檢表暨工作底稿

| **序號** | **領域** | **評估細項**  | **符合** | **未符合** | **不適用** | **說明** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 組織 | 是否已指派組織及部門內負責個人資料管理的人員? |  |  |  |  |
| 2 | 組織 | 是否已組成個人資料保護組織，並清楚說明維護本公司內部個人資料之管理作業權責? |  |  |  |  |
| 3 | 組織 | 承上題，上述要求是否已有文件化，載明成立個人資料保護管理組織及角色，並配置相當資源? |  |  |  |  |
| 4 | 組織 | 是否配置個資保護聯絡窗，負責個資當事人行使個人資料相關權利及提出相關申訴與諮詢? |  |  |  |  |
| 5 | 組織 | 是否已確認組織內部有關個人資料之蒐集 、處理 、利用之範圍? |  |  |  |  |
| 6 | 組織 | 是否訂定經組織核准之個人資料管理政策，說明並要求個人資料將如何被蒐集、處理、利用、以及保護? |  |  |  |  |
| 8 | 告知 | 本公司依法向當事人直接蒐集個資時，是否明確說明蒐集個人資料的機關名稱、目的 、個資類別、期間、地區、對象、處理方式/當事人行使權利及方式/不提供之影響?  |  |  |  |  |
| 9 | 告知 | 本公司是否提供清楚與明顯的說明有關個人資料的安全維護方式? |  |  |  |  |
| 10 | 告知 | 本公司是否提供清楚與明顯的說明有關當事人如何查詢或存取其個人資料? |  |  |  |  |
| 11 | 告知 | 本公司是否提供清楚與明顯的說明有關當事人如何更正或刪除其個人資料? |  |  |  |  |
| 12 | 告知 | 本公司內間接蒐集之個人資料是否已規劃告知當事人? |  |  |  |  |
| 13 | 告知 | 本公司是否設計提供當事人申訴程序與管道? |  |  |  |  |
| 14 | 蒐集處理利用 | 本公司是否有盤點公司內所有的個人資料檔案，並建立清冊以利管理? |  |  |  |  |
| 15 | 蒐集處理利用 | 本公司內是否針對各項個人資料之蒐集、處理、利用及銷毀建立資料管制流程確保個人資料的保護? |  |  |  |  |
| 16 | 蒐集處理利用 | 本公司進行個人資料蒐集時是否遵循所屬主管機關的規定或管理辦法? |  |  |  |  |
| 17 | 蒐集處理利用 | 本公司內是否識別間接蒐集之個人資料之利用的適法性及與蒐集特定目的之合關聯? |  |  |  |  |
| 18 | 蒐集處理利用 | 本公司是否合法進行特種個資(病歷、醫療、基因、性生活、檢康檢查、犯罪前科)蒐集、利用及處理? |  |  |  |  |
| 19 | 蒐集處理利用 | 本公司若有蒐集特種資料是否符合合法蒐集的要件? |  |  |  |  |
| 21 | 蒐集處理利用 | 本公司若有蒐集特種資料,是否有適當之安全維護計畫? |  |  |  |  |
| 22 | 蒐集處理利用 | 本公司之個人資料管理是否有建立必要之使用紀錄、軌跡資料(Log Files) 及證據之保存措施? |  |  |  |  |
| 23 | 蒐集處理利用 | 本公司內是否有針對個人資料進行盤點及進行風險評估? |  |  |  |  |
| 24 | 蒐集處理利用 | 本公司內是否有針對個人資料不同等級處理進行安控措施(含備份檔案及軌跡檔案) |  |  |  |  |
| 25 | 蒐集處理利用 | 本公司之是否執行資料安全管理? |  |  |  |  |
| 26 | 蒐集處理利用 | 本公司之是否執行人員安全管理? |  |  |  |  |
| 27 | 蒐集處理利用 | 本公司之是否執行設備安全管理? |  |  |  |  |
| 28 | 蒐集處理利用 | 本公司之是否有針對個人資料顯示進行適當的去識別化? |  |  |  |  |
| 29 | 蒐集處理利用 | 本公司與其他部門個人資料交換是否已識別個人資料之適法性及特定目的利用之合理性? |  |  |  |  |
| 30 | 蒐集處理利用 | 本公司與其他部門個人資料交換是否已採取適當保護措施? |  |  |  |  |
| 31 | 蒐集處理利用 | 對於個資(紙本及數位資料)之存取及利用是否保有完整的紀錄、軌跡資料? |  |  |  |  |
| 32 | 蒐集處理利用 | 本公司是否已針對受委託處理個資案件之部門,於契約上訂有個資保護法令及機關內部個資相關規定要求? |  |  |  |  |
| 33 | 蒐集處理利用 | 本公司是否已針對受委託的公司或第三方，於契約上訂有明確監督要求?並執行監督? |  |  |  |  |
| 34 | 蒐集處理利用 | 本公司是否有將資料進行國際傳輸，並評估是否符合目的事業主管機關對國際傳輸的管理規定? |  |  |  |  |
| 35 | 蒐集處理利用 | 本公司是否以逕行有效的個人資料保護全面性(含新人)人員宣導及教育訓練? |  |  |  |  |
| 36 | 訓練 | 本公司是否針對負責管理及維護個人資料檔案之個資專人進行有效的專業教育訓練? |  |  |  |  |
| 37 | 程序 | 本公司是否已建立個人資料內管理程序或規則，以確保部門內個人資料蒐集、處理、利用刪除及傳輸符合特定目的的要求? |  |  |  |  |
| 38 | 程序 | 本公司是否有設計及執行當事人查詢、變更、刪除資料之程序? |  |  |  |  |
| 39 | 程序 | 本公司是否有設計當發生個人資料被竊取、洩漏、竄改或其他受害者事件之主動通知程序? |  |  |  |  |
| 40 | 程序 | 本公司是否有設計及執行風險評估及管理程序? |  |  |  |  |
| 41 | 程序 | 本公司是否有設計及執行個資事故通報及應變處理程序? |  |  |  |  |
| 42 | 程序 | 本公司是否有設計及執行內部稽核程序? |  |  |  |  |
| 43 | 程序 | 本公司是否有設計及執行當個人資料蒐集目的消失或屆滿之資料刪除程序? |  |  |  |  |
| 44 | PDCA | 本公司對於個資之蒐集、處理與利用之流程,是否進行內部稽核? |  |  |  |  |
| 45 | PDCA | 本公司是否定期檢視個資保護政策及個資保護執行結果? |  |  |  |  |
| 56 | PDCA | 本公司是否有實施個人資料安全維護之整體持續改善計畫? |  |  |  |  |

稽核人員：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 附件十、稽核報告書

OO年度 內部稽核報告書

報告日期:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 報告人(內部稽核小組管理代表)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| 稽核範圍 |  |
| 稽核日期 |  |
| 稽核地點 |  |
| 稽核人員 |  |
| 受稽人員 |  |
| 稽核項目 |  |
|  稽核結果：  |
|  總結建議： |
| 稽核人員 |  |
| 個資管理代表 |  |

# 附件十一、矯正預防單

矯正預防單

|  |  |  |  |
| --- | --- | --- | --- |
| 編號 |  | 年月日 |  |
| 矯正措施執行部門 |  | 措施負責人(部門負責人) |  | 提出不符合事項人 |  |

|  |  |
| --- | --- |
| **矯正計畫** | 「不符合內容」(記載為內部稽核發現不符合的事實、跡證、人員、時間等) |
|  |
| 「原因」(記載稽核發現點發生的根本原因) |
|  |
| 提出計畫日期: |  | 核決計畫日期: |  |
| 提出計畫人:(部門負責人) |  | 計畫核決人:(個人專人或部門主管) |  |
| 預定執行矯正措施完畢日期: |  | 是否需要確認矯正措施:□ 是 □ 否 |
| **矯正措施執行結果** | **執行矯正措施 內容** |
|  |
| 執行完畢日期: |  | 核決日期: |  |
| 提出計畫人:(部門負責人) |  | 計畫核決人:(個資專人或部門主管) |  |
| **審核** | **確認矯正措施效果及有效性** |
|  |
| 執行日期: | 核決日期: |  |
| 報告人: | 個資管理代表 |  |

# 附件十二、銷毀申請單

**紀錄銷毀申請單**

表單編號：(紀錄保管人員於存檔時編號)

|  |  |
| --- | --- |
| 申 請 部 門 |  |
| 申 請 人 員 |  |
| 申 請 日 期 | 年 月 日 |
| 表 單 編 號 |  |
| 銷 毀 資 訊 | 起訖流水號 \_\_\_\_\_\_\_\_\_\_\_\_\_~\_\_\_\_\_\_\_\_\_\_\_\_\_\_起迄日期 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_~\_\_\_\_\_\_\_\_\_\_\_\_\_\_數量 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 銷 毀 方 式 |  |
| 委外銷毀陪同人員 | (委外銷毀始需填寫此欄位) |
| 委外銷毀廠商 | (委外銷毀始需填寫此欄位) |
| 銷毀日期 | 年 月 日 |
| 紀錄保管人員 | 委外銷毀陪同人員 | 部門主管 |
|  | (委外銷毀始需簽核此欄位) |  |

註：若委外執行銷毀，紀錄保管人員應確認相關陪同紀錄已附於此表單，始得存檔。

# 附件十三、個資事件通報單

|  |
| --- |
| **個人資料侵害事故通報與紀錄表**  |
| 業者名稱  通報機關   | 通報時間: 年 月 日 時 分通報人: 簽名(蓋章) 職稱: 電話: Email: 地址:  |
| 事件發生時間  |   |
| 事件發生種類     | □竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害事故  | 個人資料侵害之總筆數(大約)  筆  |
| □一般個人資料\_\_\_\_\_\_\_\_\_\_ 筆 □特種個人資料\_\_\_\_\_\_\_\_\_\_ 筆  |
| 發生原因及事件摘要  |   |
| 損害狀況  |   |
| 個人資料外洩可能結果  |   |
| 擬採取之因應措施  |   |
| 擬採通知當事人之時間及方式  |   |
| 是否於知悉個人資料外洩後72小時通報  | □是 □否，理由：   |