中興保全科技股份有限公司

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

文件編號	PI-PRC-01
版　　次	1.8
機密等級	一般
發行日期	2024/01/29

版本修訂紀錄表

文件版本	制/修訂日期	內容說明	發行者
V1.0	2015/07/20	新制定	資訊事務室
V1.1	2015/12/31	組織調整	資訊事務室
V1.2	2016/12/23	因應個資法修法、主管機關頒訂「保全業個人資料檔案安全維護管理辦法」及 105 年度風險處理計畫	總執行長室
V1.3	2018/09/07	組織調整	總執行長室
V1.4	2019/08/20	公司名稱及組織調整	總執行長室
V1.5	2020/03/19	組織調整	服務企劃室
V1.6	2021/05/07	文件更名:個人資料風險評鑑作業說明	服務企劃室
V1.7	2022/02/10	因應主管機關頒訂「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」	服務企劃室
V1.8	2024/01/29	因應組織調整，修正、調整程序內容	資安管理室

目錄

第壹章 總則

一、 制定目的

中興保全科技股份有限公司(以下簡稱本公司)為落實個人資料之保護及管理，確保本公司在蒐集、處理或利用個人資料時，皆能尊重當事人之權益，並於特定目的之必要範圍內，依誠實信用方法為之，且與蒐集之目的具有正當合理之關聯，因此依據：

(一) 本公司個人資料保護最高指導原則【個人資料管理政策】之規劃；

(二) 我國【個人資料保護法】(以下簡稱【個資法】) 、【個資法施行細則】、【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】及其他相關法律，訂定本公司【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)，作為本公司個人資料管理體系執行個人資料安全維護措施之規範。

二、適用範圍

本計畫及處理方法適用於：依據本公司【個人資料管理政策】、【個資法】、【個資法施行細則】、【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】或其他要求而納入本公司個人資料管理體系之個人資料相關作業(包括蒐集、處理或利用等…)。

三、名詞定義

(一) 個人資料：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、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。

(二) 特種個人資料：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。

(三) 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

(四) 蒐集：指以任何方式取得個人資料。

(五) 處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

(六) 利用：指將蒐集之個人資料為處理以外之使用。

(七) 當事人：指個人資料之本人。

第貳章 個人資料管理政策

四、 個人資料管理政策(以下簡稱本政策)為本公司之個人資料保護管理最高指導原則，本公司同仁均應共同遵循。本政策如下：

(一) 確保本公司符合我國個人資料保護法、個資法施行細則、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，及主管機關函令等要求。

(二) 保障個人資料當事人之隱私權，並提供管道供其行使個人資料之自主權。

(三) 對個人資料之蒐集、處理及利用過程，當以誠實及信用方法為之，不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。

(四) 規劃並提供個人資料檔案適當之安全措施，以確保本公司善盡監督管理之注意義務。

第參章 管理人員及資源配置

五、 管理組織架構、資源配置與職掌

(一) 本公司設立個人資料保護管理組織，以配置管理之人員及相當資源，負責規劃、訂定、修正及執行本計畫及處理方法等相關事項，並依本公司【個人資料管理組織暨權限管理要點】定期審查各項個人資料安全維護措施執行成效。

(二) 本公司【個人資料管理政策】公告於中興保全科技資料庫入口【個資保護專區】，提供本公司各層級人員及駐點人員查閱；並於官方網站首頁提供連結，提供客戶知悉本公司蒐集、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。

(三) 總公司轄下各分公司亦應遵循本計畫及處理方法之各項要求。

第肆章 個人資料之範圍界定

六、 納入管理之個人資料範圍

(一) 本公司應識別所保有之個人資料檔案，及蒐集、處理、利用個人資料之流程，劃定其納入本計畫及處理方法之範圍，並依本公司【個人資料檔案盤點作業標準與說明】建立並維護「個人資料檔案清冊」。

(二) 依據「個人資料檔案清冊」納入本公司本計畫及處理方法之管理範圍，應評估其隱私權衝擊程度，以確保納入管理之個人資料適用並符合【個資法】相關規範。

(三) 隱私權衝擊評估方法依據 BS10012:2017 條文，並採用 General Data Protection Regulation（簡稱 GDPR）個人資料使用的六大原則，說明如下：

1. 正確性：

   針對當事人對於其個人資料的合理期待，針對可能損及當事人權益的風險，應採取適當的風險處理措施以避免損害。

2. 公開透明性：

   必須以「合法」、「公平」、「透明」手段來蒐集、處理個人資料。

3. 目的拘束性：

   必須以明確、合法的目的來蒐集個人資料。

4. 儲存限制性：

   不得逾越處理個資目的的必要範圍，並在資料儲存期間做合理保管。

5. 機密性：

   必須以資安手段確保個人資料不被破壞或散佈。

6. 資料最小化：

   必須在最低限度內蒐集、使用個人資料。

(四) 個人資料及隱私保護法令遵循

1. 本公司各部門之個人資料聯繫窗口應定期整理並更新業務相關法令，通報法令遵循單位/人員以協助評估其適用性及符合性；遇有法令變更或新增時，各部門亦應立即通報法令遵循單位/人員。
2. 因執行業務適用之個人資料及隱私保護法令遵循發生疑義時，該部門之個人資料聯繫窗口應先通報部室主管，以暫停該業務之執行，並向法令遵循單位/人員通報業務內容、所適用之法令及其適用上之疑義，待法令遵循單位確認後方得續行該業務。
3. 上述個人資料及隱私保護之「適用法令遵循列表」之說明與確認，應作成紀錄並由資安管理室保管並歸檔。

第伍章　個人資料之風險管理

七、　個人資料之風險評估及管理機制

本公司應就納入本計畫及處理方法範圍之個人資料，鑑別本公司因蒐集、處理、利用個人資料可能面臨的風險，並依本公司【個人資料風險評鑑作業說明】進行個人資料風險評估，視重大作業風險審查結果，規劃及執行個人資料安全維護方案。

第陸章　個人資料事故之預防、通報及應變機制

八、　事前預防作業

個人資料管理體系維護小組(以下簡稱個資小組)事前預防作業要點如下：

(一) 應將個人資料於發生被竊取、竄改、毀損、滅失、洩漏等個資事故之緊急應變處理，依本公司風險管理及危機處理作業原則等相關規範，訂定包括危機任務編組、應變策略、公關溝通及善後處理標準等作業流程之【個人資料事故緊急應變處理計畫】。

(二) 應統籌本公司各單位(得包含總公司轄下各分公司或辦事處)透過教育訓練或實際演練驗證【個人資料事故緊急應變處理計畫】之有效性，並與風險管理架構相結合，對於處理後之重大作業風險仍高於可容忍程度之事項，應預先規劃危機之預防、應變及復原各階段因應措施。

九、事故通報

(一) 本公司各單位獲報來自客戶、員工或其他當事人之個人資料相關案件時，應初步確認其屬：

1. 個資外洩事件通報；
2. 個人資料當事人權利行使，

若確定為個資外洩事件，應立即以電話、電子郵件或其他適當方式，通報至總公司個資小組之受理通報窗口，並由個資小組依【個人資料事故緊急應變處理計畫】辦理；若為個人資料當事人權利行使，則依本計畫處理方法第捌章「當事人權利行使作業」規定辦理。

(二) 非上班時間應通知本公司客服中心，客服中心獲報後應即依據本公司通報相關程序辦理，並通報個資小組窗口。

(三) 對外通報須知：於個資事故確認後，以適當方式通知利害關係人；如遇有達五千筆以上之個人資料事故時，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、是否於發現個人資料外洩後立即通報等事項，依【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】指定格式，通報當地直轄市或縣（市）主管機關，並副知中央主管機關。

十、事故應變

(一) 本公司個資小組於接獲通報後，除協調相關單位、技術支援廠商及諮詢機關辦理外，應由主要權責及其他相關單位依事故等級，由資安長指派成立事故緊急應變單位/人員。

(二) 事故緊急應變單位/人員應辦理下列事項：

1. 應於接獲通報後即刻進行事故分析。事故分析應包含確認事故之種類、事故嚴重程度、影響的範圍以及發生原因。
2. 於事故分析後，應研擬事故應變處理措施避免事故擴大，並採取證據保全措施，避免異動或改變原始磁碟及證據。
3. 於事故查明後，應即適當方式通知當事人被侵害之事實以及已採取之措施。適當方式得依以言詞、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使當事人知悉或可得悉之方式為之。

十一、媒體應對

本公司各單位於個資事故發生後，應注意媒體報導，如與論關注須對外說明及澄清，說明內容經資安長及總執行長核准後，由公司發言人適時召開記者會或發布新聞稿說明。

十二、復原及矯正

(一) 本公司個資小組及各單位應於完成事故應變後，重新檢討事故發生之原因並擬定改善計劃；必要時，得重新進行風險評估、規劃個人資料安全維護措施或設計個人資料管理體系。

(二) 事故緊急應變單位/人員應將事故檢討及改善計劃，製作個資事故處理報告書，送交資安管理室備查。

(三) 個人資料事故之預防、通報及應變作業若有未完善之事項，請依本計畫及處理方法第壹拾貳章 「內部稽核、紀錄保存及持續改善」，執行矯正及預防措施作業之程序。

(四) 直轄市、縣（市）主管機關對於本公司重大個人資料事故，依【個人資料保護法】第二十二條規定對本公司之應變、通報及預防機制進行實地檢查，本公司將依檢查結果辦理後續處置事宜，以配合中央主管機關督導直轄市、縣（市）主管機關對於本公司之相關機制改善情形。

第柒章 個人資料檔案蒐集、處理與利用作業

十三、合法蒐集

(一) 蒐集個人資料時，應先辨識該業務項目蒐集個人資料之目的及個人資料之類別，並符合本公司業務項目之特定目的，確認其合法性，除有下列情形之一者外，不得為之：

1. 法律明文規定。
2. 與當事人有契約或類似契約之關係，且已採取適當之安全措施。
3. 當事人自行公開或其他已合法公開之個人資料。
4. 經當事人同意。
5. 為增進公共利益所必要。
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。
7. 對當事人權益無侵害。

(二) 無法判斷是否符合蒐集個人資料之合法性要件時，可向個資法令遵循單位/人員確認。

(三) 蒐集個人資料時，應留存相關證明文件與紀錄，證明蒐集之合法性。

(四) 各部門因執行業務所必要或新增業務項目，而有蒐集個人資料之新需求時，經個資法令遵循單位/人員評估其適法性後方得蒐集。

十四、告知義務

(一) 告知踐行：

1. 直接蒐集之告知事項：

   蒐集直接由當事人提供之個人資料時，應於取得時明確告知當事人下列事項，同時留存告知之紀錄。但法令規定免告知者，不在此限：

(1) 本公司名稱。

(2) 蒐集之目的。

(3) 蒐集個人資料之類別。

(4) 個人資料利用之期間、地區、對象及方式。

(5) 當事人依個人資料保護法第三條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，不提供將其權益之影響。

2. 間接蒐集之告知事項：

蒐集非由當事人直接提供之個人資料時，應於首次處理或利用前或於利用時，向當事人告知個人資料來源及前項第一款至第五款所列事項。

(二) 無法判斷是否符合“直接/間接蒐集個人資料之應告知事項”時，告知之權責單位應向個資法令遵循單位/人員確認其適法性後，方可踐行告知。

(三) 告知之方法與紀錄

1. 對當事人告知時，應以數位或書面方式為之，但法令另有規定得免告知時，不在此限。

2. 書面進行告知時，應參酌「個人資料蒐集告知條款」，於契約書、申請書、通知書、委託書及其他文件中載明應告知之事項。

3. 向當事人踐行告知義務時，應依照告知方法留存相關紀錄，其保存期限至少五年或等同於所蒐集個人資料之保存期限。

(四) 免告知情況

經各部室主管判斷為下列情形時，得免為告知：

1. 向當事人蒐集個人資料，得免為告知情形如下：

(1) 依法律規定得免告知。

(2) 個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。

(3) 告知將妨害公務機關執行法定職務。

(4) 告知將妨害公共利益。

(5) 當事人明知應告知之內容。

(6) 個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響。

2. 蒐集非由當事人提供之個人資料，除符合前點 (1) ~ (6) 情形外，有下列情形之一者，得免為告知：

(1) 當事人自行公開或其他已合法公開之個人資料。

(2) 不能向當事人或其法定代理人為告知。

(3) 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

3. 各部室主管無法判斷是否符合得免告知之情形，應以書面提報至個資法令遵循單位/人員，確認是否符合得免告知之要件。

十五、處理及利用個人資料

(一) 各單位內因業務必要而處理或利用個人資料時，應於特定目的之必要範圍內為之，並與蒐集之目的具有正當合理之關聯。

(二) 個人資料之最小化原則如下：

1. 應確認僅蒐集聲明範圍內執行業務所需之個人資料。

2. 處理及利用時應僅使用所需之最小化個人資料。

3. 應確認不處理與特定目的範圍無關或不必要之個人資料。

(三) 利用個人資料係交與第三方單位做為活動用途或提供查調資料時，應確認其符合本計畫及處理方法（十二、合法蒐集及十三、告知義務）、相關法令及主管機關之要求，始得提供資料。另應注意下列事項：

1. 個人資料交與第三方單位如做為活動用途，與第三方單位簽署之契約、發函或聲明文件等，應載明雙方權利義務，並採取適當程序要求個人資料之使用有適當保護，且不踰越當事人同意之範圍。

2. 個人資料如須提供查調資料予第三方時，須留存提供紀錄備查。

(四) 個人資料之保存除法令另有規定外，各部門應訂定合理保存期限。

(五) 對於處理或利用之行為是否符合蒐集之特定目的有疑義時，應先暫停其處理或利用行為，並以書面向個資法令遵循單位/人員確認符合蒐集之目的後，方得開始處理或利用個人資料。

十六、特定目的外利用

(一) 除有下列情形之一，不得將個人資料為特定目的外之利用：

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. 經當事人同意。
7. 有利於當事人權益。

(二) 對個人資料為特定目的外之利用時，應先填具「個人資料“特定目的外利用”申請表」，向個資法令遵循單位/人員申請。個資法令遵循單位/人員應確認“特定目的外利用”下列檢核事項：

1. 利用之資料來源。
2. 目的內利用原則。
3. 告知義務(明確告知當事人特定目的外之其他利用目的、範圍及同意與否對其權益之影響)。
4. 資料保存方式/存放地點。
5. 行銷原則。
6. 利用之安全維護。

(三)「個人資料“特定目的外利用”申請表」檢核結果，應經該單位主官會簽、資安管理室資安長核准，並由個資法令遵循單位/人員留存相關紀錄。

(四) 各部門有(一)之情形時，該個人資料為特定目的外利用經核准後，應將利用過程作成紀錄，並將利用之資訊依本要點相關規範，將其個人資料納入本公司個人資料管理體系之範圍，建立並維護其個人資料檔案清冊。

十七、商業行銷

(一) 利用個人資料進行行銷時，應先判斷原先蒐集之特定目的是否包括行銷，原先蒐集之特定目的並未包括行銷時，應先依特定目的外利用程序辦理，方得執行後續行銷作業。

(二) 利用個人資料首次行銷時，應告知當事人得拒絕接受行銷，並免費提供當事人表示拒絕接受行銷之方式。

(三) 當事人表示拒絕接受行銷者，應立即停止利用其個人資料行銷。

(四) 利用個人資料行銷時，應留存相關紀錄。

十八、特種個人資料

(一) 有關病歷、醫療、基因、性生活、健康檢查、犯罪前科之個人資料，除業務必要並符合下列情形之一者外，不得蒐集、處理或利用：

1. 法律明文規定（包括法律及法律具體明確授權之法規命令)。
2. 本公司履行法定義務所必要，且有適當安全維護措施（事前或事後)。
3. 當事人自行公開或其他已合法公開之個人資料。
4. 本公司為協助公務機關執行法定職務或非公務機關履行法定義務所必要，且有適當安全維護措施（事前或事後)。
5. 本公司已取得當事人書面同意者，但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

(二) 無法判斷是否符合蒐集、處理或利用特種個人資料之合法性要件時，應以書面提報至個資法令遵循單位/人員，確認是否符合得使用特種個人資料之要件。

(三) 部門內因業務必要而蒐集、處理或利用有關病歷、醫療、基因、性生活、健康檢查、犯罪前科之個人資料時，應留存相關證明文件，以證明蒐集、處理或利用之合法性，並規劃適當安全維護措施及留存相關紀錄。

十九、內部及外部傳輸

傳輸個人資料檔案予其他部門或第三方時，應依照檔案機密等級採行適當之安全措施和程序，以及依照「個人資料安全及實體環境管理辦法」辦理，並留存相關簽收紀錄或寄件備份。

二十、國際傳輸

(一) 對個人資料為國際傳輸時，應依本要點處理及利用之規定為之，並確保個人資料於國（境）外之使用均有控管並留存相關紀錄。

如有下列情形之一者，不得為之：

1. 涉及國家重大利益。
2. 國際條約或協定有特別規定。
3. 接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。
4. 以迂迴方法向第三國（地區）傳輸個人資料以規避個人資料保護法。

(二) 本公司將個人資料作國際傳輸者，應確認是否受到中央主管機關限制，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：

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【個人資料保護法】第三條所定權利之相關事項。

二十一、 刪除、停止處理或利用個人資料

(一) 個人資料檔案保存之特定目的消失或期限屆滿時，各部門應依公司規定進行刪除/銷毀作業，並保留下列相關紀錄。

1. 刪除、停止處理或利用之方法、時間或地點。
2. 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。

(二) 前述 1.、2.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。

(三) 委託他人進行銷毀作業時，應進行相關監督或稽核作業，並作成相關紀錄。

(四) 有下列情形之一者，應以停止蒐集、處理及利用個人資料之方式代替銷毀或刪除，並規劃適當保有該個人資料檔案安全維護措施，避免造成該個人資料目的外利用：

1. 有法令規定或契約約定之保存期限。
2. 有理由足認銷毀或刪除個人資料檔案，將侵害當事人值得保護之利益。
3. 儲存方式特殊致不能銷毀或刪除或耗費過鉅者。

第捌章　委外管理

二十二、 書面約定

本公司因執行業務而委託或複委託他人蒐集、處理或利用個人資料時，應以書面為之，並約定保密、定期監督之權利及損害賠償責任。

前項監督應至少包含下列事項或參照「受委託廠商個人資料風險評估聲明書」，載明於契約書或相關書面文件：

(一) 預定蒐集、處理或利用個人資料之範圍、類別、特定目的、利用之期間、地區、對象及其方式。

(二) 受託者就【個資法】施行細則第 12 條第 2 項所列安全維護事項應採取之措施。

(三) 受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及委託契約時，應向本公司通知之事項及採行之補救措施。

(四) 本公司對受託者保留指示之事項。

(五) 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。

(六) 限非經本公司同意禁止受託者複委託之規範。

(七) 保密條款。

(八) 委託事項所涉及之個人資料檔案及其數量。

(九) 委外廠商權限之控管及定期清查檢視。

二十三、 受委託廠商之評估

(一) 委託單位應依據委外採購相關規範，考量受託者執行個人資料保護措施之狀況，並應記錄確認結果，呈相關權責主管核閱。

(二) 委託關係有自動續約時，需求部門準用前項規定。發現受託者個人資料管理未符合預期狀況之事項時，應要求受託者進行改善並提出改善成果報告。

二十四、 委外業務關係終止或解除

(一) 委託業務關係終止或解除時，應要求受託者依約定方式確實刪除、銷毀或返還因執行受託業務所保有之個人資料，並提供刪除、銷毀或返還所保有個人資料之時間、方式、地點等紀錄；必要時，得進行實地訪查確認。

第玖章　當事人權利行使作業

二十五、 當事人權利行使

當事人就其個人資料行使之下列權利，除法令另有規定外，本公司不得拒絕辦理，並提供聯絡窗口及聯絡方式：

(一) 查詢或請求閱覽。

(二) 請求製給複製本。

(三) 請求補充或更正。

(四) 請求停止蒐集、處理或利用。

(五) 請求刪除。

二十六、 當事人權利行使之受理程序

(一) 申請人直接向各部門提出行使權利之請求時，原則上應轉知客戶權利行使單位/人員，由其統一受理，並將處理結果記錄於「當事人權利行使申請單」或以其他適當方式記錄之；惟各部門若有其業務上之考量，得依本要點逕行處理，並於事件處理完畢後，將回覆結果紀錄通報予客戶權利行使單位/人員。

(二) 當事人之權利，不得要求預先拋棄或以特約限制之。

(三) 客戶權利行使單位/人員受理申請人前條第一項之請求後，受理程序如下：

1. 客戶權利行使單位/人員應立即確認申請人之身分：

   (1) 申請人為當事人時，應先核對並確認其人別。

   (2) 申請人為受當事人委託之代理人時，應確認代理人之代理權限。

2. 當事人委託他人代為行使權利者，應符合下列情形之一者：

   (1) 當事人未成年時，其法定代理人（如父母親）。

   (2) 當事人為受監護宣告或輔助宣告之人時，其監護人或輔助人。

   (3) 經當事人授權者。

3. 申請人之請求有下列情形之一者，客戶權利行使單位/人員得拒絕受理之：

(1) 當事人提出權利行使之請求，無法確認其身分時。

(2) 當事人委託他人代為行使權利，無法確認其代理權時。

(3) 申請人請求行使權利者，非係當事人之個人資料時。

(4) 申請人之請求與本公司持有之個人資料不符合時。

4. 客戶權利行使單位/人員受理申請人之請求時，應立即向當事人確認受理之項目，並於 5 個工作日內將當事人行使權利之請求移送至相關部門。

(四) 檢附之相關證明文件內容如有遺漏或欠缺，客戶權利行使單位/人員應通知申請人限期補正。

(五) 申請案件如有下列情形之一者，應以書面駁回其申請：

1. 申請書內容或相關證明文件有遺漏或欠缺，經通知限期補正後，逾期仍未補正。

2. 有個資法第 10 條但書各款情形之一。

3. 有個資法第 11 條第 2 項但書或第 3 項但書所定情形之一。

4. 與其他法令規定不符。

二十七、 當事人權利行使之處理程序

(一) 客戶權利行使單位/人員移送當事人行使權利之請求時，部室主管應於期限內為准駁之決定，並向客戶權利行使單位/人員通報處理結果：

1. 申請人請求查詢、提供閱覽或製給複製本時，部室主管應於 5 個工作日內為准駁之決定；必要時，部室主管得檢附理由向客戶權利行使單位/人員申請延長，延長之期間不得逾 5 個工作日，客戶權利行使單位/人員准予延長時，應將延長之期間及其原因以書面方式通知申請人。

2. 申請人請求補充、更正、刪除及停止蒐集、處理或利用個人資料時，部室主管應於 10 個工作日內為准駁之決定；必要時，部室主管得檢附理由向客戶權利行使單位/人員申請延長，延長之期間不得逾 10 個工作日，

客戶權利行使單位/人員准予延長時，應將延長之期間及其原因以書面方式通知申請人。

(二) 部室主管拒絕申請人之請求時，應敘明理由向客戶權利行使單位/人員通報處理結果。

(三) 申請人請求查詢、提供閱覽或製給複製本時，如有下列情形之一者，部室主管得拒絕申請人之請求：

1. 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。
2. 妨害公務機關執行法定職務。
3. 妨害本公司或第三人之重大利益（有害於該第三人個人之生命、身體、自由、財產或其他重大利益）。

(四) 申請人請求刪除、停止處理或利用個人資料時，如有下列情形之一者，部室主管得拒絕申請人之請求：

1. 有法令規定或契約約定之保存期限。
2. 有理由足認刪除將侵害當事人值得保護之利益。
3. 其他不能刪除之正當事由。
4. 經當事人書面同意者。

(五) 部室主管向客戶權利行使單位/人員通報處理結果時，應檢附相關紀錄，由客戶權利行使單位/人員保管，其保存期限至少 5 年。

二十八、 當事人權利行使之回覆程序

(一) 部室主管應向客戶權利行使單位/人員通報處理結果，客戶權利行使單位/人員應留存相關紀錄。客戶權利行使單位/人員應於 3 個工作日內回覆申請人之請求，回覆時應留存相關紀錄。

(二) 若由各部門自行回覆申請人，應於回覆後立即通報客戶權利行使單位/人員。

第壹拾章 資料安全與人員管理

二十九、 資料安全

本公司應依照「個人資料安全及實體環境管理辦法」及個人資料檔案之機密性、完整性及可用性，妥善設定並管理其個人資料使用之存取權限，過濾非權限範圍之人員使用及異動情形；傳輸及儲存方式同之。其他資料安全管理事項請參照本公司資訊安全管理規範辦理。

三十、人員管理

(一) 本公司應管理與監督個人資料相關業務之人員。人員管理方式如下：

1. 員工招募：
   (1) 招募員工必須要求應徵人員簽署「應徵人員個資告知暨同意書」。
   (2) 內部處理個資檔案之人員，應符合保密及競業禁止事項及競業禁止條款之相關規範。
   (3) 需處理個資檔案之人員，其進用及調派均有適當考慮。
2. 員工在職：
   (1) 員工應簽立「員工個人資料告知暨同意書」。
   (2) 本公司應將員工應盡之安全責任納入其管理制度文件，並對內部處理個資檔案之員工，施予資訊安全與個人資料隱私保護之教育訓練，並於單位內宣導個人資料隱私保護之重要性(認知宣導及教育訓練)。
   (3) 處理個資檔案員工職務如有異動，應將所保管之儲存媒體及個資有關資料列冊移交，接辦人員除應於相關作業系統重新設定 ID 帳號使用權限(資料安全管理)。
   (4) 員工應妥善保管個人資料之儲存媒介物，並善盡保管及保密義務。
   (5) 如違反本公司【個人資料管理政策】或相關程序/規定，則按公司現有之獎懲辦法視情節懲處。

3. 員工離職：

(1) 處理個資檔案之員工，離職時應確認其使用或保管之資訊資產是否依規定繳回或辦理移除(員工離職作業流程)。

(2) 處理個資檔案員工，離職時應確認已取消或停用其使用者 ID 帳號，且收繳其員工識別證及相關證件(員工離職作業流程)。

(3) 處理大量個資檔案之員工，離職時應稽核並確認其是否有異常的個資處理紀錄(資料安全稽核機制、設備稽核紀錄、資料庫防火牆管理)。

(4) 員工離職時，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。

(二) 本公司資訊系統使用之人員，除設定其使用權限外，應對於資料之使用與異常規劃系統紀錄機制，以利於控制與追蹤使用者之使用情形。

(三) 本公司同仁於在職及離、退職後、接觸個人資料之外部人員、委外服務廠商人員於合約終止或解除後，均不得洩漏所知悉之機密及個人資料之資訊，或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。

第壹拾壹章 認知宣導及教育訓練

三十一、 規劃與管理

(一) 個人資料保護認知宣導及教育訓練應依人員管理方式，規劃定期或依實際需求，每年至少舉辦一次，使本公司員工皆能明瞭個人資料保護相關法令及公司之規定，並於訓練完成後，作成施行紀錄，提交各部室主管會議及報告成果。

(二) 個人資料管理教育訓練結束後應將教育訓練施行紀錄發交予各部室主管，若有缺課或未達教育訓練之預定成果者，應定期限要求各部室主管提出補課名單與補課施行紀錄，並歸檔於教育訓練施行紀錄中。

三十二、 宣導及訓練內容

辦理個人資料保護認知宣導及教育訓練時，得參考下列事項：

(一) 個人資料管理之重要性及最佳實務。

(二) 個人資料管理體系中各層級人員之權責。

(三) 個人資料管理之具體執行方式。

(四) 違反個人資料管理相關規範之後果。

(五) 國際隱私保護規範趨勢。

(六) 其他相關議題。

第壹拾貳章 設備安全管理

三十三、 設備管理權責

(一) 本公司處理個人資料相關之設備管理，依本公司資訊安全管理制度及「個人資料安全及實體環境管理辦法」規定辦理，並就相關設備、環境、系統設定，訂定相對應之管理措施或機制。

(二) 電腦機房管理，委託外部機構維護者，應符合本計畫及處理方法第柒章 委外管理 之相關原則，確保妥善維護本公司個人資料安全維護相關電腦機房設備；另外，本公司應建立電腦系統中斷之緊急通報，建立完善資訊系統危機處理機制。

三十四、 設備管理方式

(一) 紙本個人資料之安全管理

1. 紙本個人資料文件或檔案之存放，應符合本公司資訊安全及文書作業相關規範辦理。檔案室、倉庫或檔案櫃，宜備有監視錄影監控並留存紀錄。
2. 各項敏感性之紙本個人資料，應施以適當的控管措施，以保全其完整性、機密性及可用性；如因業務而需拷貝複製，應確保資料僅限授權之方式使用。文件儲存、調閱及銷毀作業，依據本公司文書作業相關規範辦理。

(二) 電腦設備安全管理：

1. 電腦設備非因故障、更新等維護不得擅自變更、拆裝，亦不得擅自變更電腦作業系統。
2. 定期維護保養，確保設備的完整性及可持續使用。
3. 未報經主管同意，不得將私人資訊設備(軟、硬體)任意攜入辦公場所，或擅自安裝使用。

4. 共用網路磁碟機(NAS)或設定個人專屬資料匣，應設有密碼保護；硬碟如有壞軌須送修時，應先將送修硬碟格式化後，再請廠商送修或原廠更換。

(三) 電腦系統安全管理：

1. 電腦及相關設備不使用時，應關閉結束作業、登出，或設定螢幕保護程式等控制措施。
2. 嚴禁安裝或下載未經授權使用或來路不明之軟體。
3. 業務資料應定期執行備份，以確保資料的安全及回復。
4. 作業系統應隨時更新修正以修補系統漏洞；防毒軟體應隨時更新病毒碼或防毒元件。
5. 本公司各單位使用資通訊系統蒐集、處理或利用消費者個人資料達五千筆以上者，應採取下列資訊安全措施：
   (1) 使用者身分確認及保護機制。
   (2) 個人資料顯示之隱碼機制。
   (3) 網際網路傳輸之安全加密機制。
   (4) 個人資料檔案及資料庫之存取控制與保護監控措施。
   (5) 防止外部網路入侵對策。
   (6) 非法或異常使用行為之監控與因應機制。
6. 上述(5)、(6)所定措施，應定期演練及檢討改善。

(四) 其他安全管理：

1. 資安管理室得與外部資訊安全專家或顧問，加強聯繫、協調、相互合作及經驗分享，以適當評估本公司資訊設備可能面臨的資訊安全威脅，並據以研擬及推動資訊安全措施。

2. 資訊設備管理人員得與目的事業主管機關、資訊服務提供者及通信處理機構等，建立及維持適當之互動管道，以便在發生資訊安全事件時，能迅速獲得外部的資源協助，及時解決相關問題。
3. 本公司各單位存有個人資料之紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片或其他存放媒介物報廢汰換或轉作其他用途時，應採取適當之銷毀或防範措施，避免洩漏個人資料；委託他人執行者，本公司對受委託廠商之監督依本計畫及處理方法第柒章 委外管理 相關規定辦理

第壹拾參章 內部稽核、紀錄保存及持續改善

三十五、 內部稽核

稽核室應每半年定期或不定期稽核本計畫及處理方法之執行情形，並向負責人提出報告，並留存相關紀錄，其保存期限至少五年。

三十六、 執行矯正及預防措施作業之時機

(一) 稽核室執行內部稽核作業，發現有部分事項未符合規定或標準時。

(二) 各單位自行查核及內部其他單位提出之“不符合事項”，或雖為“觀察事項”但法令遵循單位認有必要者。

(三) 主管機關、利害關係人等，提出之不符合事項或建議改善事項。

三十七、 執行矯正及預防措施作業之程序

(一) 稽核室執行內部稽核作業或資安管理室經檢視當事人申訴或諮詢之結果報告、主管機關來函等情形，發現有部分事項未符合規定或標準時，應開立「矯正與預防處理單」要求受查部門限期改善。

(二) 開立「矯正與預防處理單」時，應說明查核缺失項目及其狀況，並要求受查部門於期限內回覆。

(三) 受查部門收到「矯正與預防處理單」時，應敘明發生缺失之原因、預定採行之矯正及預防措施及預計完成之時間，於改善措施回覆期限內回覆。

(四) 收到部門所回覆之「矯正與預防處理單」後，應於預計完成矯正及預防措施之時間安排複查，如查核缺失項目已按矯正及預防措施改善，複查人員應將複查結果紀錄於「矯正與預防處理單」中，經覆核後予以結案。

三十八、 執行矯正及預防措施作業之監督與審查

未於期限內完成矯正及預防措施或已完成但缺失仍未改善時，受查部門應敘明原因，由稽核室或資安管理室安排第二次複查；如第二次複查時，受查部門仍未於期限內完成矯正及預防措施或已完成但缺失仍未改善時，受查部門應提出說明報告，提報各部室主管會議。

三十九、 紀錄保存

本公司就執行本計畫及處理方法所定各種個人資料保護體系、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，並將其產生之文件、證據、軌跡資料應予以保存，並應至少留存五年，但法令另有規定或契約另有約定者，不在此限。相關事務由資安管理室負責管理及協助各單位規劃。

四十、持續改善

本公司就本計畫及處理方法所述之個人資料保護體系與相關個人資料安全維護措施，應將執行狀況進行審查並持續改善，以達到個人資料保護與管理之目標。

第壹拾肆章 附則業務終止後個人資料處理方法

本公司各單位於個人資料業務終止後，其所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。

四十一、 其他注意事項

(一) 本計畫及處理方法未盡事宜，悉依相關法令及本公司相關規定辦理。

(二) 本計畫經「資訊安全委員會」審議通過，經總執行長核定後實施，修正時亦同。並將本計畫及處理方法報請主事務所所在地之直轄市、縣（市）主管機關備查。本政策應以適當方式佈達本公司全體人員周知。

四十二、 相關文件、表單/範例

(一) 使用文件：

1. 【個人資料保護法】及其【個資法施行細則】。
2. 【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】。
3. 【個人資料管理政策】。
4. 【個人資料管理組織暨權限管理要點】。
5. 【個人資料檔案盤點作業標準與說明】。
6. 【個人資料風險評鑑作業說明】。
7. 【個人資料事故緊急應變處理計畫】。
8. 【個人資料安全及實體環境管理辦法】

(二) 表單、範例：

1. 適用法令遵循列表。
2. 個人資料“特定目的外利用”申請表。
3. 受委託廠商個人資料風險評估聲明書
4. 應徵人員個資告知暨同意書。
5. 員工個人資料告知暨同意書。
6. 矯正與預防處理單。
7. 個人資料蒐集告知條款
8. 當事人權利行使申請單