中華郵政股份有限公司

個人資料檔案安全維護計畫

SM-60-003

第 1.9 版

公告生效日期：110 年 12 月 22 日

交通部中華郵政股份有限公司

文件修訂沿革

發行 / 修訂 版次	發行 / 修訂 生效日期	發行與變更說明	備　　註
第 1.0 版	101 年 7 月 16 日	新版文件發行	
第 1.1 版	102 年 8 月 28 日	依金管會及銀行公會之「個人資料檔案安全維護計畫」修訂本公司「個人資料檔案安全維護計畫」內容	
第 1.2 版	103 年 4 月 30 日	依據金管會 102 年 11 月 8 日金管法字第 10200704150 號令「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」修訂	
第 1.3 版	103 年 12 月 5 日	配合 ISO 27001:2013 修訂	
第 1.4 版	104 年 5 月 4 日	調整文字敘述	
第 1.5 版	104 年 7 月 31 日	根據金管會 104 年 7 月 3 日金管法字第 10400914910 號令修訂	
第 1.6 版	104 年 12 月 17 日	根據交通部 104 年 9 月 24 日交郵字第 1040502398 號函辦理。	
第 1.7 版	105 年 11 月 2 日	依據個資法修正、金管會 105 年 5 月 25 日金管保綜字第 1052562221 號令，調整文字敘述。	

第 1.8 版	110 年 11 月 24 日	依據交通部 110 年 11 月 2 日交郵字第 1105014057 號函辦理。	
第 1.9 版	110 年 12 月 22 日	依據金管會 110 年 12 月 14 日金管法字第 11001966241 號令修訂。	

目　　錄

壹、目的

中華郵政股份有限公司（以下簡稱本公司）依據個人資料保護法（以下簡稱本法）第二十七條第一項規定，應訂定適當之安全維護措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏，且依據同條第二項授權中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫，確保個人資料之安全維護。故參照「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」及交通部 104 年 9 月 24 日交郵字第 1040502398 號函，訂定本公司個人資料檔案安全維護計畫（以下簡稱本計畫），以維護本公司所保有之個人資料檔案安全。

貳、範圍

本計畫適用於本公司個人資料保護管理體系內之業務及其業務相關部門，應如何適切遵循本法要求蒐集、處理及利用該業務個人資料檔案。

參、權責

一、董事會

核可本計畫之實施。

二、資訊安全暨個人資料保護管理委員會

(一) 覆核個人資料保護管理推動小組所提之本計畫。

(二) 裁決重大資訊安全暨個人資料保護管理議題。

三、個人資料保護管理推動小組

(一) 視實際需要檢討及修正本計畫。

(二) 規劃、訂定、修正與執行個人資料檔案安全維護計畫相關程序。

四、個人資料管理代表

個人資料保護管理推動小組召集人係為本公司個人資料管理代表，為使事業負責人本公司總經理能盡其督導及監督之責，個人

資料管理代表應定期向資訊安全暨個人資料保護管理委員會報告個人資料保護管理推動執行情形。

五、內評小組

負責監督或評核本計畫之執行成效。

肆、名詞定義

一、個人資料

依本法第二條第一款之規定，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。

二、特種個人資料

依本法第六條之規定，指有關自然人病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

三、本公司所屬人員

執行業務之過程必須接觸個人資料之人員，包括本公司正式人員、約聘（僱）人員、工讀生、志工等。

四、同意

依本法第七條之規定，第十五條第二款及第十九條第一項第五款所稱同意，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示；第十六條第七款、第二十條第一項第六款所稱同意，指當事人經蒐集者明確告知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後，單獨所為之意思表示;第六條第一項第六款所稱同意為經當事人書面同意。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。

五、書面同意

書面同意為本公司採取以紙本或符合電子簽章法之電子文件方式為之。

六、儲存媒體

係指各類保存個人資料之各類媒介，包含紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、電腦、自動化機器設備或其他媒介物。

七、電子商務

係指透過網際網路進行有關商品或服務之廣告、行銷、供應、訂購或遞送等各項商業交易活動。

伍、參考文件

一、金融監督管理委員會「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」。

二、交通部104年9月24日交郵字第1040502398號函。

三、金融監督管理委員會「保險法第一百七十七條之一第二項所定本人書面同意方式、業務範圍及其他應遵行事項管理辦法」(金管會105年5月25日金管保綜字第1052562221號令)。

四、交通部110年11月2日交郵字第1105014057號函。

陸、作業內容

一、管理組織之建立及配置相當資源

本公司為規劃、訂定、修正與執行本計畫，建立個人資料保護管理組織，並配置管理之人員及相當資源。前項管理組織及其任務如下：

(一) 資訊安全暨個人資料保護管理委員會

1. 擔任全公司資訊安全暨個人資料保護管理之最高決策、指導及仲裁之常設性任務編組單位。
2. 為重大資訊安全暨個人資料保護事務之提案、討論。
3. 裁決重大資訊安全暨個人資料保護管理議題。
4. 覆核個人資料保護管理推動小組所提之本計畫。

(二) 個人資料保護管理推動小組

1. 協助資訊安全暨個人資料保護管理委員會執行與維護個人資料保護事項。
2. 規劃、訂定、修正與執行個人資料檔案安全維護計畫相關程序。
3. 個人資料保護管理推動小組召集人係為本公司個人資料管理代表，為使本公司總經理能盡其督導及監督之責，管理代表應定期向資訊安全暨個人資料保護管理委員會報告個人資料保護管理推動執行情形。
4. 個人資料保護管理推動小組下設內評小組，負責監督或評核本計畫之執行成效。

二、個人資料保護管理政策

本公司應依據組織與事業特性訂定個人資料保護管理政策，經本公司總經理核可，並公開周知，使本公司所屬人員均明確瞭解。上述政策至少應包括下列事項：

(一) 遵守我國個人資料保護相關之法令規定。

(二) 以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。

(三) 以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。

(四) 設置聯絡窗口，供當事人行使關於個人資料之權利或提出相關之申訴與諮詢。

(五) 處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。

(六) 如有委託蒐集、處理及利用個人資料時，妥善監督受託機關。

(七) 持續維運本計畫，以確保個人資料檔案之安全。

三、個人資料之識別

本公司應依據個人資料保護相關法令，定期清查所保有之個人資料現況，界定其納入本計畫之範圍並建立清冊。

四、風險評鑑

本公司應根據前項所界定之個人資料範圍，及其相關業務涉及個人資料蒐集、處理、利用之流程，分析可能產生之個人資料風險。並根據風險評估之結果，訂定適當之管控措施，以確認受管控之風險在可接受範圍內。

五、事故之應變、通知及預防程序

本公司為因應所保有之個人資料被竊取、竄改、毀損、滅失或洩漏等事故，應訂定下列程序：

(一) 事故發生時應採取適當之應變措施，包括：

1、控制事故對當事人損害之方式。

2、查明事故後通知當事人之適當方式。

3、應通知當事人事故事實、所為因應措施及諮詢服務專線等內容。

4、於事故發生後 72 小時內通報中央目的事業主管機關，或通報直轄市、縣(市)政府，同時副知中央目的事業主管機關。

(二) 通報內容應包含非公務機關名稱、通報人及聯絡方式、通報主管機關、通報時間、事件發生時間、擬通知當事人之時間、事件發生種類、個資類型、預估個資侵害總筆數、發生原因、損害狀況、個資侵害可能結果、擬採取之因應措施、擬採通知當事人之方式。

(三) 查明事故之狀況並適時通知當事人、主管機關及有關單位等受通報之對象。

(四) 事故發生後其矯正預防機制之研擬，以避免類似事故再次發生。

(五) 本公司如發生重大個人資料安全事故，包含個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及本公司正常營運或大量當事人權益之情形，應依據影響當事人之範圍立即通報主管機關，並由公正、獨立且取得相關公認認證資格之專家，針對所研議之改善措施協助進行整體診斷及檢視。

六、委託蒐集、處理及利用個人資料之監督程序

本公司委託他人蒐集、處理或利用個人資料之全部或一部時，為對受託人為適當之監督，應依據本法施行細則第八條於委託契約或相關文件中，明確約定下列要求：

(一) 確認所委託蒐集、處理或利用之個人資料之範圍、類別、特定目的及其期間。

(二) 確認受託人應採取必要安全措施。

(三) 有複委託者，確認其複委託對象。

(四) 受託人或其受僱人違反個人資料保護法令或委託契約條款時，要求其向委託人通知相關事項。

(五) 與受託人約定委託人所保留指示之事項。

(六) 委託關係終止或解除時，要求受託人返還或銷毀因委託事項所交付之個人資料載體，及刪除因委託事項所儲存於受託人之個人資料。

(七) 確認受託人執行上述要求事項之狀況。

七、個人資料蒐集、處理及利用之內部管理與法令遵循程序

(一) 個人資料蒐集應注意事項及告知義務履行

1. 本公司為確保個人資料之蒐集符合個人資料保護相關法令要求，應建立下列程序：

(1) 確認所蒐集、處理及利用之個人資料是否包含本法第六條所定之特種個人資料，檢視其特定目的及是否符合相關法令之要件。

(2) 確認個人資料蒐集、處理是否符合本法第十九條規定，具有特定目的及法定情形。

(3) 確認資料蒐集、處理及利用如必須取得當事人同意者，應符合本法第七條之規定取得當事人同意，惟對當事人同意之事實負舉證責任。

(4) 確認如按保險法規定蒐集、處理或利用病歷、醫療、健康檢查等特種個資時，書面同意應符合下列要求：

A、書面同意之內容，至少應包含當事人同意就其本人之病歷、醫療、健康檢查之個人資料，所為允許蒐集、處理或利用之意思表示。

B、書面同意得獨立為之或列入要保書、理賠文件或其他相關文件，應有獨立欄位清楚標示或以適當方式使當事人得以知悉書面同意之內容。

C、為特定目的外之利用者，其書面同意並應有獨立簽署之欄位使當事人得以知悉其內容並確認同意。

D、不得有誤導、引人錯誤或要求當事人拋棄或限制個人資料保護法相關權利之敘述。

2. 本公司為遵守本法第八條及第九條關於告知義務之規定，應建立下列程序：

(1) 確認個人資料之蒐集、處理是否得符合免告知之事由。

(2) 依據資料蒐集之情況，採取合法且妥適之告知方式與內容。

(二) 確保於特定目的內利用個人資料及特定目的變更之程序

1. 本公司為確保個人資料之利用符合個人資料保護相關法令要求，應建立下列程序：

(1) 確保個人資料之利用符合特定目的。

(2) 於特定目的外利用個人資料時，應確認是否符合本法第二十條第一項但書所定情形，得進行及如何進行特定目的外利用。

2. 本公司對其所保有之個人資料進行特定目的之新增或變更時，應先確認依法是否得為之，並應依據新增或變更之目的，確認其符合法令之要求，並再次履行告知義務。

(三) 利用個人資料行銷之程序

本公司於利用個人資料行銷時，應建立下列程序：

1. 確認當事人是否願意接受行銷，並留存紀錄。

2. 確保當事人表示拒絕接受後，立即停止利用其個人資料行銷，並通知資料處理相關單位。

3. 於首次行銷時，提供當事人免費表示拒絕接受行銷之方式。

(四) 國際傳輸之程序

本公司為國際傳輸個人資料時，應建立是否受中央目的事業主管機關依本法第二十一條規定所限制之確認程序，如有限制國際傳輸之命令或處分，應遵守之。

八、當事人權利行使

(一) 本公司為提供資料當事人行使本法第三條所規定之當事人權利，應建立下列程序：

1. 提供當事人行使權利之方式，並告知所需支付之費用，及應釋明之事項。
2. 確認當事人身分之方式。
3. 對當事人請求之審查方式，並遵守本法有關處理期限之規定。
4. 確認是否有本法第十條及第十一條所定得拒絕當事人行使權利之情況，其理由記載及通知當事人之方式。

(二) 為使當事人有效行使其權利，提供一定方式，如常設聯絡窗口，包含聯絡電話或聯絡之電子郵件信箱等，即為首要之程序。

(三) 避免資料不當提供給第三人或不當刪除，提供當事人行使權利前，應先建立確認當事人身分程序。

(四) 應於本法所規定時限內，適時回覆當事人請求。

(五) 本公司為確認保有之個人資料處於正確且最新之狀態，應建立下列程序：

1. 確保個人資料於蒐集、處理或利用過程，正確性不受影響。
2. 個人資料有錯漏時，應適時主動或依當事人之請求更正或補充資料。
3. 個人資料正確性有爭議時，應主動或依當事人之請求停止處理、利用。有繼續利用之必要者，應註明其爭議或取得當事人書面同意之程序。
4. 因可歸責於本公司之事由，未為更正或補充之個人資料，應建立於更正或補充後，通知曾提供利用對象之程序。

(六) 本公司應定期確認其所保有個人資料之特定目的是否消失，或期限是否屆滿，如特定目的消失或期限屆滿時，應遵守本法第十一條第三項規定，訂定刪除或停止處理利用之程序，並留存執行紀錄。

1. 檢視所保有個人資料之特定目的是否消失，或期限是否屆滿。
2. 檢視特定目的已消失或期限已屆滿之個人資料，是否為執行業務所必須。有繼續處理、利用之必要者，須取得當事人書面同意之方式。

3. 刪除、停止處理或利用之方式與通知曾提供利用對象之程序。

九、安全管理措施

為防止個人資料發生被竊取、竄改、毀損、滅失或洩漏等遭受侵害之情事，本公司應依據業務性質、個人資料存取環境、個人資料種類與數量及個人資料傳輸工具與方法等因素，採取下列管理措施：

(一) 人員管理

1. 確認蒐集、處理及利用個人資料之相關業務流程負責人員。
2. 依據作業必要，設定所屬人員不同權限並控管，以一定認證機制管理，且定期確認權限內容設定之適當與必要性。
3. 與本公司所屬人員簽訂保密契約，契約內容至少包含本公司所屬人員應負保密義務與保密範圍，及違反保密義務效果。
4. 本公司應定期對於本公司所屬人員施以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要求、所屬人員責任範圍及各種個人資料保護事項之機制、作業程序。

(二) 作業管理

1. 訂定蒐集、處理及利用之作業注意事項。
2. 運用電腦或自動化機器等設備蒐集、處理或利用個人資料時，應訂定各類設備或儲存媒體之使用規範。
3. 各類設備及儲存媒體之安全管理措施應包含存取管制、保存方式，並依媒體之特性及其環境建置適當之保護設備或技術。
4. 針對所保有之個人資料內容，確認是否有加密之必要，如有必要，應採取適當加密機制。
5. 傳輸個人資料時，因應不同傳輸方式，確認是否有加密必要，如有必要，應採取適當加密機制，並確認資料收受者之正確性。
6. 本公司應依據所保有資料之重要性，評估個人資料是否有備份必要，如有必要應予備份，並比照原件，依本法規定予以保護。對於備份資料應確認是否有加密之必要，如有必要，

應採取適當加密機制，儲存備份資料之媒體亦應以適當方式保管，且定期進行備份資料還原測試，以確保備份有效性。

7. 各類設備或儲存個人資料之媒體於廢棄或移轉他用前，應確實刪除媒體中所儲存之資料，或以物理方式破壞等防範資料洩漏之適當措施。
8. 妥善保存認證機制及加密機制中所運用之密碼，如有交付他人之必要，亦應妥善為之。
9. 提供或顯示個人資料時，應考量針對與業務無關之個人資料內容，提供隱碼等去識別化機制。

(三) 實體安全管理

1. 依據作業內容之不同，實施必要之門禁管理，如：人員進出管制、錄影監控。
2. 妥善保管個人資料之儲存媒體。
3. 針對不同作業環境，建置必要之防災設備。

(四) 技術管理

1. 於電腦、相關設備或系統上設定認證機制，對有存取個人資料權限之人員進行識別與控管。
2. 認證機制使用帳號及密碼之方式時，使其具備一定安全之複雜度並定期更換密碼。
3. 於電腦、相關設備或系統上設定警示與相關反應機制，以對不正常之存取為適當之反應與處理。
4. 對於存取個人資料之終端機進行身分認證，以識別並控管之。
5. 個人資料存取權限之數量及範圍，於作業必要之限度內設定之，且原則上不得共用存取權限。
6. 採用防火牆或路由器等設定，避免儲存個人資料之系統遭受無權限之存取。
7. 欲使用能存取個人資料之應用程式時，確認使用者具備使用權限。
8. 定期測試權限認證機制之有效性。
9. 定期檢視個人資料之存取權限設定正當與否。

10. 於處理個人資料之電腦系統中安裝防毒軟體，並定期更新病毒碼。
11. 對於電腦作業系統及相關應用程式之漏洞，定期安裝修補之程式。
12. 定期瞭解惡意程式之威脅，並確認安裝防毒軟體及修補程式後之電腦系統之穩定性。
13. 具備存取權限之終端機不得安裝檔案分享軟體。
14. 測試處理個人資料之資訊系統時，不使用真實之個人資料，如有使用真實之個人資料之情形時，明確規定其使用之程序。
15. 處理個人資料之資訊系統如有變更時，確認其安全性並未降低。
16. 定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形。
17. 本公司針對電子商務服務系統，除上述控管外應另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去識別化機制。
    (3) 系統開發、上線、維護等各階段軟體驗證與確認程序。
    (4) 網際網路傳輸之安全加密機制。
    (5) 個人資料檔案及資料庫之存取控制與保護監控措施。
    (6) 外部網路入侵防護與演練。
    (7) 非法或異常使用行為之監控與因應機制。

十、計畫實施與持續改善

(一) 計畫實施

本計畫之訂定，應經董事會通過後公告實施，並授權個人資料保護管理推動小組視實際需要檢討修正之。

(二) 計畫稽核及改善程序

1. 本公司為確保本計畫之有效性，應訂定適當之個人資料安全稽核及自我評估機制，定期檢查本計畫是否落實執行，並向個人資料管理代表提出評估報告。
2. 應建立計畫發生未落實執行之情形時，規劃執行改善及預防之程序。

(三) 計畫持續更新

1. 本公司因其業務種類、特性及其所蒐集、處理、利用之個人資料範圍之不同與變動，其所應適用之個人資料保護法令亦可能有所不同，為符合法令之規定，應依據上述業務自身狀況清查適用之個人資料保護相關法令。
2. 個人資料保護相關法令規定，因時事變遷而有隨之變更之可能，本公司應定期檢視所應遵循之個人資料保護相關法令，以持續修訂其安全維護計畫。
3. 本公司將持續維運本計畫，以確保個人資料檔案之安全。

十一、文件紀錄管制

(一) 本公司為確保本計畫各項程序之執行，應記錄個人資料使用情形、留存軌跡資料或相關證據，至少應保存下列紀錄，相關證據及紀錄至少留存五年，但法令另有規定或契約另有約定者，不在此限：

1. 因應事故發生所採取行為之紀錄。
2. 確認受託人執行委託人要求事項之紀錄。
3. 提供當事人行使權利之紀錄。
4. 確認資料正確性及更正之紀錄。
5. 權限新增、變動及刪除之紀錄。
6. 違反權限行為之紀錄。
7. 備份及還原測試之紀錄。
8. 個人資料交付、傳輸之紀錄。
9. 個人資料刪除、停止處理或利用之紀錄。
10. 存取個人資料系統之紀錄。
11. 定期檢查處理個人資料之資訊系統之紀錄。
12. 教育訓練之紀錄。

13. 計畫稽核及改善程序執行之紀錄。

(二) 本公司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：

1. 刪除、停止處理或利用之方法、時間。

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，及該對象蒐集、處理或利用之合法依據。

柒、輸出文件/紀錄

無。

捌、個資檢查表

項次	項　　目
1.	本公司是否設立資訊安全暨個人資料保護管理委員會、個人資料保護管理推動小組，並配置管理之人員及相當資源，以執行個人資料檔案安全維護計畫？
2.	本公司個人資料保護管理推動小組召集人，是否定期向事業負責人以書面報告管理執行情形？
3.	本公司是否依據組織與事業特性訂定個人資料保護管理政策，經本公司負責人核可，並公開周知，使本公司所屬人員均明確瞭解？

4.	本公司個人資料保護管理政策是否包含下列事項： (一) 本公司將遵守我國個人資料保護相關之法令規定。 (二) 本公司將以合理安全之方式，於特定目的範圍內，蒐集、處理及利用個人資料。 (三) 本公司將以可期待之合理安全水準技術保護其所蒐集、處理、利用之個人資料檔案。 (四) 本公司將會設置聯絡窗口，供當事人行使關於個人資料之權利或提出相關之申訴與諮詢。 (五) 本公司將以妥善方式處理個人資料被竊取、竄改、毀損、滅失或洩漏等事故。 (六) 如有委託蒐集、處理及利用個人資料時，本公司將妥善監督受託機關。 (七) 本公司將持續維運本計畫，以確保個人資料檔案之安全。
5.	本公司是否根據前項所界定之個人資料範圍，及其相關業務涉及個人資料蒐集、處理、利用之流程，分析可能產生之個人資料風險，並根據風險評估之結果，訂定適當之管控措施，以確認受管控之風險在可接受範圍內？
6.	本公司是否已訂定個人資料事故發生時應採取適當之應變措施，以控制事故對當事人之損害擴大？
7.	本公司是否已訂定個人資料事故發生後，查明事故之狀況並適時通知當事人、主管機關及有關單位等受通報之對象等處置程序？
8.	委託他人蒐集、處理或利用個人資料之全部或一部時，是否於委託契約或相關文件中明確約定下列要求： (一)確認所委託蒐集、處理或利用之個人資料之範圍、類別、特定目的及其期間。 (二)確認受託人應採取必要安全措施。 (三)有複委託者，確認其複委託對象。 (四)受託人或其受僱人違反個人資料保護法令或委託契約條款時，要求其向委託人通知相關事項。 (五)與受託人約定委託人所保留指示之事項。 (六)委託關係終止或解除時，要求受託人返還或銷毀因委託事項所交付之個人資料載體，及刪除因委託事項所儲存於受託人之個人資料。 (七)確認受託人執行上述要求事項之狀況。
9.	個人資料蒐集、處理是否符合本法第十九條規定，具有特定目的及法定情形？如為經當事人同意而得蒐集、處理個人資料者，是否符合本法第七條第一項之規定？

10.	個人資料蒐集、處理及利用如必須取得當事人同意者，是否符合本法第七條之規定，蒐集者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後，單獨所為之意思表示？
11.	個人資料之蒐集、處理是否確認得符合免告知之事由，或採取合法且妥適之告知方式與內容？
12.	對其所保有之個人資料進行特定目的之新增或變更時，是否先確認依法得為之，並是否依據新增或變更之目的，確認其符合法令之要求，再次履行告知義務？
13.	本公司於利用個人資料行銷時，是否確認當事人是否願意接受行銷，並留存紀錄？
14.	是否建立當事人權利行使之程序？包含： (1)當事人行使權利之方式。 (2)確認當事人身分之方式。 (3)對當事人請求之審查方式。 (4)拒絕當事人行使權利之情況時，理由記載及通知當事人之方式。
15.	是否確保個人資料於蒐集、處理或利用過程，正確性不受影響？
16.	個人資料正確性有爭議時，是否應主動或依當事人之請求停止處理、利用？有繼續利用之必要者，是否註明其爭議或取得當事人書面同意之程序？
17.	是否定期確認其所保有個人資料之特定目的是否消失，或期限是否屆滿？如特定目的消失或期限屆滿時，是否訂定刪除或停止處理利用之程序，並留存執行紀錄？如有繼續處理、利用之必要者，是否取得當事人書面同意之方式？
18.	是否與本公司所屬人員簽訂保密契約，契約內容至少包含本公司所屬人員應負保密義務與保密範圍，及違反保密義務效果？
19.	針對所保有之個人資料內容，是否確認有加密之必要，如有必要，是否採取適當加密機制？
20.	傳輸個人資料時，因應不同傳輸方式，是否確認有加密必要，如有必要，是否採取適當加密機制，並確認資料收受者之正確性？
21.	是否依據作業內容之不同，實施必要之門禁管理？
22.	是否妥善保管個人資料之儲存媒體？
23.	個人資料存取權限之數量及範圍，是否於作業必要之限度內設定之？且原則上不得共用存取權限？
24.	於電腦、相關設備或系統上是否設定認證機制，對有存取個人資料權限之人員進行識別與控管？認證機制使用之密碼是否具備一定安全之複雜度並定期更換？

25.	處理個人資料之電腦系統中是否安裝防毒軟體，並定期更新病毒碼？
26.	電腦作業系統及相關應用程式之漏洞是否定期安裝修補之程式？
27.	具備存取權限之終端機是否不得安裝檔案分享軟體？
28.	是否定期檢查處理個人資料之資訊系統之使用狀況及個人資料存取之情形？
29.	是否定期檢視所應遵循之個人資料保護相關法令，以持續修訂其安全維護計畫？
30.	是否持續維運個人資料檔案安全維護計畫，以確保個人資料檔案之安全？
31.	是否記錄個人資料使用情形、留存軌跡資料或相關證據，以確保本計畫各項程序之執行？

個人資料侵害事故通報與紀錄表

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</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>事件發生時間</td><td colspan="2"></td></tr>
<tr><td rowspan="2">事件發生種類</td><td rowspan="2">□竊取
□洩漏
□竄改
□毀損
□滅失
□其他侵害事故</td><td>個資侵害之總筆數(大約)
_____</td></tr>
<tr><td>□一般個資 _____筆
□特種個資 _____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資外洩可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩後72小時通報主管機關</td><td colspan="2">□是　□否，理由</td></tr>
</table>

註1：各欄位資訊若尚未明確，得先填寫「不明」，並俟明確後再通報更新補充。

註2：上開72小時通報主管機關(如金融監督管理委員會等)，例假日均納入時效計算。