元大保全股份有限公司個人資料檔案安全維護計畫

111 年 01 月 02 日訂定
113 年 05 月 01 日修正一版

第一條　依內政部 110 年 11 月 3 日台內警字第 11008786931 號函「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」訂定本公司「個人資料檔案安全維護計畫」。

第二條　本法主管機關為新北市政府(警察局)，經律訂後報請主管機關新北市政府(警察局)備查。

第三條　元大保全股份有限公司（以下簡稱本公司）為維護個人資料檔案安全，特依據內政部所令頒之「個人資料檔案安全維護管理辦法」，訂定本公司之個人資料檔案安全維護計畫，以防止員工個人資料遭竊取、竄改、毀損或洩漏。

第四條　本公司組織規模

一、 組織型態：股份有限公司
二、 資本額：新台幣肆仟萬元整
三、 公司地址：新北市三重區成功路 147 號 2 樓
四、 代表人(負責人)：林正銘

第五條　本公司就現有員工之個人資料由人事部門統一集中保管，並由各事業部門將個人資料予以分類保管，且設置專櫃儲存；有關安全維護管理依據內政部所頒「保全業個人資料檔案安全維護管理辦法」第六條至第二十二條規定，訂定適當之個人資料檔案安全維護管理措施，本計畫包括如後：

一、 配置管理人員方面及資源：

本公司人事部門編制檔案維護主管乙位、檔案管理員 1 位，負責規劃、訂定、修正與執行個人資料檔案安全維護計畫以及業務終止後之個人資料安全處理等相關事項，並定期向負責人提出報告。

二、 蒐集、處理與利用個人資料範圍：

(一) 資料蒐集與利用之目的：保全服務、行銷、契約或類似契約或其他法律關係事務、消費者客戶管理與服務、人事管理、採購與供應管理。

(二) 客戶個人資料：本計畫所稱之客戶個人資料，除係指客戶姓名、出生年月日、國民身分證統一編號、婚姻、家庭、教育、職業、聯絡方式外及其他得以直接或間接方式識別該個人之資料。

(三) 面試人員與員工個人資料：指姓名、出生年月日、身分證統一編號、婚姻、家庭、職業、健康檢查、財產狀況、聯絡方式等，及其他得以直接或間接識別該個人之資料。

三、 風險評估與管理機制

(一) 風險評估

1. 經由本公司電腦下載或外部網路入侵而外洩。

2. 經由接觸客戶書面契約書類而外洩。
3. 經由接觸人事個資紙本檔案而外洩。
4. 總公司與分公司、各區營業處或各事業部門間或受委託之公司或商業間互為傳輸時外洩。
5. 因員工故意竊取而導致毀損或外洩。

（二） 管理機制

1. 藉由使用者代碼、識別密碼設定及文件妥適保管。
2. 定期進行網路資訊安全維護及控管。
3. 電磁資料視實際需要以加密方式傳輸。
4. 書面契約、紙本資料之傳輸或者調閱應有檔案維護管理員記錄在冊並嚴加把關傳輸與調閱者之身分與用途。
5. 加強對員工之管制及設備之強化管理。

四、 個人資料蒐集、處理及利用之內部管理措施

（一） 直接向當事人蒐集個人資料時，應明確告知以下事項：

(1) 公司名稱
(2) 蒐集目的
(3) 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) 當事人得請求閱覽、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
(6) 當事人得自由選擇提供個人資料時，不提供將對其權益有影響之資料

（二） 所蒐集非由當事人提供之個人資料，應於處理或利用前向當事人告知個人資料來源及前項應告知之事項。

（三） 與客戶或員工簽訂之契約書(保全契約或員工勞動契約)，完成履行、解除或終止時，除因執行職務或業務所必須或經客戶或員工書面同意者，應於法規規定之須留存年限後主動刪除或銷毀，並留存相關紀錄。

（四） 利用個人資料為行銷時，當事人表示拒絕行銷後，應立即停止利用其個人資料行銷。

（五） 客戶或者員工表示請求閱覽、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，告知連絡窗口為：邱小姐 ；電話為：02-6637-2088。並將聯絡窗口及電話等資料，揭示於本公司營業處所或公司網頁。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。

（六） 負責保管及處理個人資料檔案之人員，其職務有異動時， 應將所保管之儲存媒體及有關資料檔案移交，以利管理。

（七） 由指定之管理人員定期清查所保有之個人資料是否符合蒐集特定目的，若有非屬特定目的必要範圍之資料，或特定目的消失、期限屆滿而無保存必要者，即予刪除、銷毀或其他適當處置。

（八） 本公司如有委託他人蒐集、處理或利用個人資料時，應依個人資料保護法施行細則第八條規定對受託者為適當之監督並明確約定監督事項及方式。

（九） 所蒐集之個人資料如需作特定目的外利用，必須先行檢視是否符合個人資料保護法第二十條第一項但書規定。

（十） 本公司因故終止業務時，原保有之個人資料，即依規定不再使用，並採銷毀、移轉或其他妥適方式處理。

（十一） 如中央主管機關依個人資料保護法第二十一條規定，對保全業為限制國際傳輸個人資料之命令或處分時，本公司應通知所屬人員遵循辦理。

五、 事故之預防、通報及應變機制

（一） 預防

1. 本公司員工或各事業單位人員如因其工作執掌而須輸出、輸入個人資料時，需向人事部門主管提出申請，經由檢核確認有必要時為之；相關管理人員在輸出或者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. 非承辦之人員參閱契約書類時應向公司負責人、總經理或經指定之管理人員提出申請，經同意後為之。

3. 個人資料於總公司與各分公司或者各事業部間互為傳輸時，加強管控避免外洩。

4. 加強員工教育宣導，並嚴加管制。

（二） 通報及應變機制

1. 發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向公司負責人通報，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客戶或者員工，應儘速以適當方式或書面通知使其知悉，並告知本公司所採取之處理措施及聯絡電話窗口等資訊。

3. 針對事故發生原因研議改進措施。

4. 發生重大個人資料事故時，立即以書面通報新北市政府警察局。

六、 資料安全管理、人員管理及設備安全管理

（一） 資料安全管理

1. 電腦存取個人資料之管控：

(1) 個人資料檔案儲存在電腦硬式磁碟機上者，應在個人電腦設置識別密碼、保護程式密碼或相關安全措施。

(2) 個人資料檔案使用完畢應即退出，不得任其停留於電腦螢幕上。

(3) 定期進行電腦系統防毒、掃毒之必要措施。

(4) 重要個人資料應另加設管控密碼，非經陳報單位主管核可，並取得密碼者，不得存取。

2. 紙本資料之保管：

(1) 對於各類契約書件及個人資料表應指定專人管理並存放於公文櫃或檔案室內並上鎖，員工非經權責主管核可不得任意複製或影印。

(2) 對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

（二） 人員安全管理

1. 本公司依業務需求，適度設定所屬人員（如主管、非主管人員）不同之權限，以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。

2. 本公司個資檔案管理人員每三個月應變更識別密碼 1 次，並於變更識別密碼後始可繼續使用電腦。

3. 本公司員工應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。

4. 員工離職時，應刪除離職人員電腦權限。其因執行業務所持有之個人資料應辦理交接，不得在外繼續使用，並簽訂保密切結書（如在任職時之相關勞務契約已有所約定時，亦屬之）。

5. 本公司與員工或者客戶所簽訂之相關勞務契約或承攬契約均列入保密條款，以確保其遵守對於個人資料內容之保密義務。

（三） 設備安全管理

1. 建置個人資料之有關電腦、自動化機器相關設備、可攜式設備，於保養維護或更新設備時，並應注意資料之備份及相關安全措施。

2. 建置個人資料之個人電腦，不得直接作為公眾查詢之前端工具。

3. 重要個人資料備份應異地存放，並應置有防火設備或門禁系統等防護設備，以防止資料滅失或遭竊取。

4. 電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，應檢視該設備所儲存之個人資料是否確實刪除。

七、 資料安全稽核機制

（一） 本公司每半年定期或不定期辦理個人資料檔案安全維護稽核，查察本公司是否落實本計畫規範事項，針對查察結果不符合事項及潛在不符合之風險，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，向本公司負責人報告，並留存相關紀錄，其保存期限至少五年。

八、 使用記錄、軌跡資料及證據保存

本公司應採行適當措施，留存個人資料使用紀錄、自動化機器設備之軌跡資料或其他相關之證據資料，其保存期限至少五年。

九、 認知宣導及教育訓練

（一） 本公司應定期或不定期對本公司所屬人員施以個資保護之基礎認知宣導或專業教育訓練，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。

（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

（一） 本公司將隨時依據計畫執行狀況，注意相關技術發展及法令修正等事項，檢討本計畫是否合宜，並予必要之修正。

（二） 針對個資安全稽核結果有不符合法令之虞者，規劃改善與預防措施。

十一、 業務終止後之個人資料處理方法

本公司業務終止後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄，並保存五年以上：

（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。

第六條 本公司為因應個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故（以下簡稱個人資料事故），訂定下列應變、通報及預防機制：

一、 個人資料事故發生後採取之各類措施，包括：
（一）控制當事人損害之方式。
（二）查明個人資料事故後通知當事人之適當方式。

（三）通知當事人個人資料事故事實、所為因應措施及諮詢服務專線等內容。

二、 個人資料事故發生後應受通報之對象及其通報方式。

三、 個人資料事故發生後，其矯正預防措施之研議機制。

本公司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，以書面通報新北市政府警察局，並副知內政部警政署（書面通報格式如附件一）。

第七條 本公司如遇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：

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、個人資料檔案及資料庫之存取控制與保護監控措施。

五、防止外部網路入侵對策。

六、非法或異常使用行為之監控與因應機制。

前項第五款及第六款所定措施，應定期演練及檢討改善

第八條 本計畫依規定呈報新北市政府(警察局)備查，並隨時參酌業務及計畫執行狀況予修正，如有增修訂亦同。

第九條 本辦法自發布日施行。

附件一　個人資料事故通報與紀錄表

<table>
<tr><td colspan="3">個人資料事故通報與紀錄表</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>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>擬採取之因應措施 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，係指有關病歷、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，係指特種個人資料以外之個人資料。

說明：依據第八條第二項規定，定明內政部指定警政類非公務機關遇個人資料侵害事故發生後，應依本表格式通報主事務所所在地之直轄市、縣發生後，應依本表格式通報主事務所所在地之直轄市、縣(市)主管機關主管機關。