台灣新光保全股份有限公司個人資料檔案安全維護計畫

壹、保全業之組織規模

一、組織型態：股份有限公司

二、資本額：新臺幣 3,836,530,750 元整

三、公司地址：台北市內湖區行愛路 128 號

四、代表人（負責人）：林伯峰

五、員工人數：約 1,800 人

貳、個人資料檔案之安全維護管理措施

一、配置管理之人員及相當資源

（一）管理人員：

1、配置人數：特成立「個資法因應小組」，由總經理指定召集人及執行秘書各一人，其餘成員為各本部協理。

2、職責：負責規劃、訂定、修正與執行計畫或業務終止後個人資料處理方法等相關事項。

（二）預算：每一年約新臺幣 200 萬元。

（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、竄改、毀損、滅失或洩漏。

二、界定蒐集、處理及利用個人資料之範圍

（一）特定目的：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）個人資料：本計畫所稱之個人資料，係指自然人(如:客戶、員工等)之姓名、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、風險評估及管理機制

（一）風險評估

1、經由本公司或各營業處所電腦下載或外部網路入侵而外洩。

2、經由接觸書面契約書類而外洩。

3、本公司與各營業處所間或受委託之公司或商業間互為傳輸時外洩。

4、員工故意竊取、竄改、毀損或洩漏。

（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或透過加密通道傳送。

4、加強對員工之管制及設備之強化管理。

四、事故之預防、通報及應變機制

（一）預防：

1、本公司員工如因工作執掌而須輸出、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、非承辦之人員參閱契約書類時應經指定之管理人員之同意。

3、個人資料於本公司與各營業處所間或受委託之公司或商業間互為傳輸時，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：

1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏即向本公司指定之管理人員通報，並立即查明發生原因及責任歸屬，依實際狀況採取必要措施。

2、對於個人資料遭竊取之客戶，應儘速以適當方式通知使其知悉，並告知本公司已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，立即以書面通報當地直轄市或縣（市）主管機關。

五、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、 蒐集之目的。

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，不提供將對其權益之影響。

（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。前述告知事項，得於首次對當事人利用時併同為之。

（三）與客戶簽訂之保全契約完成履行、解除或終止時，除因執行職務或業務所必須或經客戶書面同意者，應主動刪除或銷毀，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）當事人表示拒絕行銷或請求閱覽、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，聯絡窗口為本公司客服中心，（如為本公司員工個人資料，聯絡窗口為本公司人資部），聯絡電話為：0800-668-850，並將聯絡窗口等資料公告於本公司，如有網站者，並揭露於網頁。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。

（七）本公司員工如因其工作執掌相關而須輸出、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，其中識別密碼並應保密，不得洩漏或與他人共用。

（八）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、銷毀或其他停止蒐集、處理或利用等適當之處置，並留存相關紀錄。

（九）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。

（十）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。

（十一）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

六、設備安全管理、資料安全管理及人員管理措施

（一）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。

（二）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，非經本公司權責主管核可，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。

（三）人員管理措施

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、本公司檢視各相關業務之性質，指派人員負責規範個人資料蒐集、處理及利用等流程。

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、本公司與員工所簽訂之相關勞務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。

6、本公司員工每三個月應變更識別密碼一次，並於變更識別密碼後始可繼續使用電腦。

七、認知宣導及教育訓練

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。

八、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，應規劃改善與預防措施，並確保相關措施之執行。

（二）前項稽核結果應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。

九、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。

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，社會輿情、技術發展及相關法令修正等事項，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。