|  |
| --- |
| **(草案範例)請各公司參考，並依公司實況撰擬訂定。** |

**○○保全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**

一、依據：

依「保全業個人資料檔案安全維護管理辦法」及內政部110年11月3日台內警字第11008786931號函規定，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」。

二、目的：

為落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

三、個人資料檔案安全維護管理措施：

(一)本公司組織規模依工作類別及任務特性，設置董事長(總經理)、副董事長(副總經理)，下設內勤(業務部：總務、人事、會計)，外勤(勤務部：勤務隊、機動小組、稽核小組)，分屬內勤與外勤經理，負責指導、協調、調度與指揮，達整體團隊相互支援共同體，個人資料檔案之安全維護及管理由內勤業務部人事承辦人員負責。

(二)個人資料檔案之安全管理：

1.公司由副總經理負責規劃、訂定、修正及執行計畫或業務終止後個人資料處理方法等相關事項，並定期向負責人提出報告。

2.個人資料檔案之安全維護及管理由內勤業務部人事承辦人負責，並專檔專櫃儲存，內勤(業務部)經理每日負督促作業情形，副總經理負責審查及簽核。

3.錄取之員工個人資料（包含家庭狀況、連絡電話、身份背景等）由人事檔案員將個人資料建立人事電腦系統內，並分類各事業部門人資，俾利檔案管理。

4.依據個人資料保護管理之政策，將蒐集、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，公告於公佈欄內，並用公司網站揭露於網站首頁，使所屬人員及個人資料當事人均能知悉。

5.人事（檔案）管理人員需確實遵守本辦法規定，嚴禁對非相關人員透漏員工個人資料，若有洩漏個資之情形，將依個人資料保護法第41條規定辦理。

6.個人資料安全維護之整體作業及規劃，人事系統檔案需建立密碼，除承辦人員使用外，任何人不得任意操作，檔案人員應定期及不定期檢查有無缺失，一經發現有作業上之問題，應即採取因應作為，以防堵資料外洩之情形。

7.對於個人之彙整及處理及利用個人資料之類別及範圍，每季清查所保管個人資料檔案之現況。清查發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，人事（檔案）管理人員並應留存相關紀錄。

8.業務終止後之個人資料之處理，統一造冊登錄後銷毀，並由副總經理監督。

9.在蒐集個人資料，應遵守本法第八條及第九條有關告知義務之規定，並區分個人資料屬直接蒐集或間接蒐集，分別訂定告知方式、內容及注意事項，要求勤務主管及人事（檔案）管理人員確實辦理。

10.為確實保護個人資料之安全，對勤務主管人事（檔案）管理人員應採取適度管理措施。

a.依據業務需求，適度設定所屬人員不同之權限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。

b.檢視各相關業務之性質，規範個人資料蒐集、處理及利用等流程之負責人員。

c.勤務主管、人事（檔案）管理人員，應確實妥善保管個人資料之儲存媒介物，並約定保管及保密義務。

d.勤務主管及人事（檔案）管理人員離職時，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。

11.對於個人資料蒐集、處理及利用，應符合本法第十九條及第二十條相關規定，並定期或不定期對於所屬人員施以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。

四、設備管理方面

(一)對所蒐集保管之個人資料檔案，應採取必要適當之安全設備或防護措施。

1.紙本資料檔案特需注意防火防潮存管，存放於上鎖鐵櫃。

2.電子資料檔案存放之電腦、可攜式設備或儲存媒體，配置安全防護系統或加密機制。

3.存有個人資料之紙本、磁碟、光碟片、或其他存放媒介物報廢汰換，銷毀時應造冊列管，業務經理需再嘗監督，避免洩漏個人資料。

(二) 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，不得任意移動電腦設備。

(三) 指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經業務經理同意並作成紀錄不得攜帶外出或拷貝複製。

(四)建立備援制度，對於重要或須永久保留之備份，有異地存放、專用防火或其他保險設施等。

(五)更新或維修電腦設備時，指定專人在場，確保個人資料之安全及防止個人資料外洩。

(六)電腦設備報廢或不使用時，確實刪除電腦硬體設備中所儲存之個人資料檔案。

五、資料稽核方面

(一)個人資料安全維護稽核，每季由副總經理查察，以落實個人資料檔案安全管理。

(二)電腦處理個人資料時，應核對個人資料之輸入、輸出、編輯或更正是否與原檔案相符。

(三)對於造成當事人之個資外洩，除應即查明原因及追究承辦人員外，並即通知當事人，以減少對當事人之損害。

(四)對於事故發生原因及損害狀況，除採取因應防堵措施外，並責由副總經理級主管給予諮詢服務及專線。

(五)造成個人資料洩漏人事（檔案）管理人員，應研議改進措施，避免類似事故再度發生。

(六)發生重大個人資料事故者，應即以書面通報新北市政府警察局主管機關。(如附件)

六、其他安全維護事項

(一)以電腦處理個人資料檔案之人員，其職務有異動時，應將其所保管之檔案資料移交，接辦人員應另行設定密碼，以利管理。

(二)保全業務終止後，保有之個人資料不得繼續使用，銷毀之方法、時間、地點須造冊登記及證明銷毀之方式拍照存證，其保存至少五年。

(三)本計畫依規定呈報新北市政府警察局備查，如有增修訂亦同。

七、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。