統超保險經紀人股份有限公司

資訊安全政策

2025/07/01 版

一、目的

統超保險經紀人股份有限公司(以下簡稱本公司)為確保營運及服務提供流程中之資訊機密性、完整性及可用性，特訂定本辦法。所有資訊使用者人員需依循此資訊安全政策進行營運及服務之資訊管理。

二、適用範圍

(一)適用於本公司及所屬單位。

(二)公司應考量其所面臨之內部與外部議題、利害相關團體對資訊安全相關的要求事項、以及公司所執行的活動與由其他組織執行活動間之相依性，訂定資訊安全管理之適用範圍以及其所面臨之風險與機會。

三、名詞定義

(一)機密性(Confidentiality)：

使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

(二)完整性(Integrity)：

保護資產的準確度（Accuracy）和完全性（Completeness）的性質。

(三)可用性(Availability)：

經授權個體因應需求之可存取及可使用的性質。

(四)資訊使用者包含本公司及所屬職員、約(聘)僱(用)人員、建置維護廠商及其他經授權使用資訊資產之相關人員。

四、權責

本公司為落實建置與管理資訊安全管理，成立「資安小組」，統籌辦理資訊安全政策、計畫執行及資源調度等事項之協調研議，該資安小組召集人組織成員擔任本小組委員，辦理及推動本公司資訊安全事宜。

五、要求事項

(一)為符合資訊安全政策，應確保：

1.資訊資產受適當的保護，防止未經授權之存取，使其機密性不被破壞；

2.資訊與資訊處理設施完整性與正確性，並保障利害相關團體(人員)之權益；

3.資訊與資訊處理設施具備高可用性，使重要業務得以持續正常運作；

4.重要業務的執行皆符合個人資料保護法之規定。

(二)資訊安全管理指標

請參考「資訊安全管理量測指標表」

(三)責任劃分

1.資安小組召集人應適時覆核，以確保對本政策之承諾與支持。
2.資安小組應適時修訂本政策，以確保本政策符合現行需求。
3.本公司高階主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾。
4.各系統管理及操作人員應透過適當程序落實本政策之要求。
5.本公司同仁、約聘（雇）人員及廠商都有責任遵循本政策。
6.本公司同仁都有責任透過適當通報機制，回報所發現之資訊安全事件或資訊安全弱點。
7.本公司同仁若有任何危及資訊安全之行為，都應該被訴諸適當之懲罰程序或法律行動。
8.資訊安全措施或規範都應符合現行法令之要求。
9.本公司同仁皆須負起持續改善資訊安全管理活動之責任。

(四)資訊安全政策評估

本政策應每年定期進行評估，以反映本公司資訊安全管理之最新狀況，確保資訊安全管理運作之可行性與有效性。

(五)資訊安全政策及規定之宣達

本政策透過公告程序，使本公司同仁及利害相關團體(人員)瞭解資訊安全政策之相關規定。

(六)公布與施行

本政策經總經理核定後實施，依實施日期起生效。修正時亦同。

(七)具體的框架/遵循要求

相關政策涵蓋之資訊安全控制範圍如下：

1.資訊資產之安全及風險管理。
2.人員安全管理及資訊安全教育訓練。
3.實體及環境安全管理。
4.個人電腦安全管理。
5.主機系統安全管理。
6.網路安全管理。
7.存取控制安全管理。
8.系統發展及維護安全管理。
9.資訊安全事故管理。
10.業務永續運作計畫之規劃及管理。
11.資訊安全稽核及遵循性管理。
12.委外安全管理。

統超保險經紀人股份有限公司

個人資料保護管理政策

2024/08/06 版

一、目的

(一)為因應社會與資訊技術之快速變遷、利害關係者之責任、義務與要求、符合相關法令規範、及與日俱增之作業環境風險，以整體風險控管之精神，決定適用範圍並建立完善之個人資料保護制度，確保本公司個人資料之蒐集、處理及利用均妥善辦理，並維護個人及其他利害關係人之利益，特制定本政策。

二、範圍

(一) 本政策適用對象：本公司全體員工(含派遣員工)及依法令規定或契約約定須適用本政策之人員或事業體。

(二) 若本政策與主管機關現行有效個人資料法令有所牴觸時，應優先適用主管機關現行個人資料保護相關法令。

(三) 就前項是否生有牴觸之爭議時，應由業務所屬部門主管提案，經個人資料保護推行小組工作會議決議，並由個人資料管理代表決定之。必要時，得委託外部法律專業人員提供書面法律意見或函請法務部釋疑。

(四) 若本公司發布之程序書與本政策有所牴觸時，應優先適用本政策。但程序書較有利於個資當事人權利之保護者，仍應適用程序書。

(五) 就前項是否生有牴觸或何者較有利於個資當事人權利保護有爭議時，應由業務所屬部門主管提案，經個人資料保護推行小組工作會議決議，並由個人資料管理代表決定之。必要時，得委託外部法律專業人員提供書面法律意見。

(六)公司應考量其所面臨之內部與外部議題、利害相關團體對個資保護相關的要求事項、以及公司所執行的活動與由其他組織執行活動間之相依性，訂定個資保護管理之適用範圍以及其所面臨之風險與機會。

三、作業說明

(一) 為符合個人資料保護管理政策，應確保下列管理目標：

1. 保護本公司業務相關個人資料之安全，避免外在威脅或內部人員不當之管理與使用，以致遭竊取、毀損、滅失、或洩漏等風險。
2. 依個人資料保護法、個人資料保護法施行細則、BS 10012 與各式合約要求，建立個人資料保護管理組織，並訂定個人資料保護管理政策與具體措施，以保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程與確保當事人權利。
3. 適時針對個人資料保護流程進行風險評鑑，以辨識公司可承受風險等級，藉以設置適切之個人資料保護措施。
4. 提升對個人資料保護與應變處理個人資料事件之能力，降低對公司營運、個資當事人與利害關係人之風險，並創造可信賴之個人資料保護及隱私環境。
5. 提升本公司員工之個人資料保護意識。

(二) 個人資料保護管理指標

請參考「資訊安全管理量測指標表」

（三）為落實個人資料保護事宜，本公司應建置個人資料保護運作組織，成立跨組織之個人資料保護推行小組，配置相當資源，並明確訂定員工在個人資料保護運作組織中之責任。

（四）本公司為界定個人資料之範圍，清查所持有個人資料檔案並建立清冊，並辨識高風險個資，且每年執行作業流程檢視及個資盤點作業，以確保、維護個人資料之正確性及從新性。

（五）本公司應建立個人資料之風險評估及管理機制，制定個人資料檔案安全維護計畫，藉由設備安全管理及人員管理，以確保本公司業務範圍內各項個資文件及檔案獲得安全保護，並確保本公司資訊系統處理個人資料之安全性、正確性與完整性。

（六）本公司應制定符合個人資料保護相關法令、主管機關之要求、組織營運目的及 BS10012 之原則之個資蒐集、處理及利用管理程序，以相當、適當、安全、公平且合法地方式，於合法特定目的範圍內，蒐集、處理（含保存）及利用最小需求之個人資料，並確保業務範圍內之個資均妥善地被管理、維護與執行，同時個資保護法所允許之例外情形亦同。且於處理直接蒐集之未成年當事人個資時，應確保該個資受到特別保護。

（七）本公司應針對合法的特定目的蒐集最少的個人資料，且僅處理相關且適當的個人資料，並明確提供個資當事人其個人資料使用方式與使用對象的資訊。

（八）個人資料之特定目的外利用，應符合個人資料保護相關法令有關例外狀況之規定。

（九）僅依據個人資料保護相關法令、主管機關要求、以及合法特定目的的要求下保存個人資料。

（十）本公司應制定業務終止後個人資料處理方法，以因應個資相關業務終止後，須移轉或銷毀之個人資料的處理方式及程序。

（十一）　本公司應建立個資遭竊取、竄改、毀損、滅失、洩漏或其他不合理或違法利用時之事故預防、通報及應變機制並適當維護個資作業流程之處理紀錄以防止個資遭受竊取、竄改、毀損、滅失、洩漏及其他不當或違法之利用，並善盡善良管理人之義務。

（十二）　本公司每年應規劃及舉辦有關個資保護之教育訓練及宣導課程，以提升本公司所有同仁對於個人資料保護之認知。

（十三）　本公司應就個人資料之蒐集、處理、利用，為必要之使用紀錄、軌跡資料及證據之保存。

（十四）　本公司應設置聯絡窗口及處理程序，供當事人行使個資法賦予之權利或提出相關之申訴與諮詢。

（十五）　本公司應明定個人資料文件及檔案之保管期限，並針對超過保管期限之文件及檔案建立刪除或銷毀等處理程序。

（十六）　本公司應僅於確定個人資料被適當保護之下，方可進行個人資料之國際傳輸。

（十七）　本公司應要求接觸本公司個資之往來廠商或業務合作對象應遵循本政策及相關規定。本公司個資相關作業委外時，應善盡委任及監督責任。

（十八）　本公司應將個資保護列入稽核檢查項目，並至少每年審查個人資料保護管理政策之執行及施行現狀，以查核個人資料保護管理制度落實狀況及矯正預防結果追蹤。

（十九） 本公司同仁如經查明確有違反本政策之情事，將依工作規則之相關懲處規定辦理。

（二十） 本公司應制定個資保護暨隱私權聲明，內容包括有關本公司對個人資料及隱私權之保護，以明確告知客戶本公司之個資暨隱私權保護相關措施，並於本公司官網上公告。

（二十一）本公司應致力發展與實施上開個人資料保護措施，並適時鑑別內外部利害關係人，及其參與個人資料保護治理之程度。