

宏遠證券股份有限公司

資訊安全政策

- 第一條 目的
為強化資訊安全管理，建立安全及可信賴之電腦及網路環境，確保資料、系統、設備、網路及個人資料安全，保障公司及客戶權益，特訂定本政策，以作為本公司資訊安全之最高指導目標。
- 第二條 資訊安全之定義
資訊安全係指將安全保護措施的規則應用於電腦系統，並使電腦系統可以正常無誤的運作。
- 第三條 範圍
相關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效：
一、人員管理及資訊安全教育訓練。
二、電腦系統安全管理。
三、網路安全管理。
四、系統存取控制。
五、應用系統開發及維護安全管理。
六、資訊資產安全管理。
七、實體及環境安全管理。
八、業務永續運作計畫之規劃與管理。
九、資訊安全稽核。
十、個人資料保護與管理。
- 第四條 原則及標準
一、個人資料保護法。
二、金融監督管理委員會發佈之證券暨期貨市場各服務事業建立內部控制制度處理準則。
三、台灣證券交易所建立證券商資通安全檢查機制及本公司內部控制制度之規定。
四、其他資訊安全相關法令。
- 第五條 員工應負一般特性及特定的資訊安全責任，並遵守政府法令及本公司制訂資訊安全相關規章之要求及規定。
- 第六條 資訊安全工作之組織、權責及分工
一、為統籌資訊安全管理等事項之協調及推動，成立資訊安全管理委員會，並由委員會召集人指派執行秘書，負責業務之執行。
二、資訊安全管理之分工原則
（一）資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由營運服務處負責辦理。
（二）資料及資訊系統之安全需求研議、管理及保護等事項，由業務單位負責辦理。
（三）資訊機密維護及安全稽核等事項，由稽核室會同相關單位負責辦理。

- 第七條 資通安全事件發生時依據緊急應變計畫暨作業處理程序處理。
- 第八條 資訊安全之評估
定期進行獨立及客觀的評估，以反映政府資訊安全管理政策、法令、技術及機關業務之最新狀況，確保資訊安全實務作業確實遵守資訊安全政策，以及確保資訊安全實務作業之可行性及有效性。
參與資訊安全的評估人員如下：
一、資訊設施及系統提供者。
二、資訊及資料擁有者。
三、使用者。
四、管理者。
五、系統維護者。
六、其他有關人員。
- 第九條 資訊安全風險評估機制
一、由資訊安全執行秘書依分工原則召集各單位，針對資產價值，弱點產生之衝擊性、威脅發生機率評估系統風險等級，決定風險可接受程度，產生風險等級評估報告，各單位依風險等級評估做處理與控制措施，將風險等級降低至風險可接受程度內。
二、風險評鑑報告，應每年至少評估乙次，並留存相關記錄。
- 第十條 資訊安全政策及規定之宣達
需以書面、電子或其他方式通知員工及與本公司連線作業之公私機構及提供資訊服務之廠商共同遵行。
- 第十一條 本政策應至少每年評估乙次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。
- 第十二條 每年應將資訊安全政策整體執行情形呈報董事會以及審計委員會。
- 第十三條 本政策之權責單位為營運服務處。
- 第十四條 本政策經董事會決議通過後施行，修正時亦同。
- 第十五條 制定及修正日期
本政策於民國九十七年十月三十日訂定。
第三次修正於民國一〇六年九月二十八日。
第四次修正於民國一〇九年一月二十日。