台中銀證券股份有限公司

資訊安全政策

103 年 2 月 11 日初版
103 年 12 月 15 日第一次修正
104 年 12 月 04 日第二次修正
105 年 12 月 30 日第 2 屆第 6 次董事會通過
106 年 12 月 5 日第 2 屆第 16 次董事會通過
107 年 12 月 10 日第 2 屆第 26 次董事會通過
110 年 11 月 19 日第 3 屆第 30 次董事會通過
111 年 11 月 18 日第 4 屆第 7 次董事會通過

第一條 目的

台中銀證券股份有限公司（以下簡稱本公司）為強化資通安全管理，確保本公司所提供資通系統開發、建置、維運及人員相關服務之資通安全，有效降低因人為疏失、蓄意或天然災害等導致之資產遭竊、不當使用、洩漏、竄改或毀損等風險，特訂定「資訊安全政策」(以下簡稱本政策)，本政策未規定事項依「資通安全管理法」及資安六子法辦理，以達成本公司資通安全之機密性、完整性、可用性與法遵性要求。

第二條 名詞解釋

本政策所稱資通安全係保護資產避免遭受各種不當使用、洩漏、竄改、竊取、破壞等事故威脅，並降低可能影響及危害業務運作之損害程度。

一、機密性 (Confidentiality)：保護敏感資訊免於未經授權公開或被他人恣意取得。

二、完整性 (Integrity)：適當之安全防護措施以防止資料不當之修改或增刪，確保資料能完整提供，未有遺漏的情形發生。

三、可用性 (Availability)：確保資訊及重要服務在使用者需要時可以取得。

四、法遵性 (Law compliance)：確保本公司各項業務服務之執行須符合相關法令規章之要求。

第三條 適用範圍

本政策適用於各項資產及資通使用者，資通使用者係包含員工、建置維護廠商及其

他經授權使用資產之人員。

第四條 依據

本政策係參考「資通安全管理法」、「建立證券商資通安全檢查機制」，並參酌資安六子法等有關法令，及 ISO 27001：2013/CNS 27001：2014 資通安全管理系統標準，考量業務需求，特訂定資訊安全政策及相關標準作業程序，以建立資通安全管理機制、強化資通安全防護，提昇資通安全之水準。

第五條 組織

為統籌資通安全管理等事項之協調、規劃、稽核及推動，參考本公司內控規範「CC-13000 安全組織」，特成立跨部門之「資訊安全推行小組」，其幕僚作業由資訊服務部負責，並依下列分工原則，配賦相關單位及人員權責：

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，由資訊安全推行小組負責辦理。

二、 資料及資通系統之安全需求研議、管理及保護等事項，由資訊服務部負責辦理。

三、 資訊安全之稽核事項，由稽核室負責辦理。

四、 資訊服務異常事件或資通安全事件，業管單位應立即通報資訊服務部及相關單位，由資訊服務部依災害狀況判斷資通安全事件等級採取反應措施。內部依規定進行通報及處理程序，若發生影響客戶權益或正常營運之資訊安全事件，應於規定時限內對外通報，相關作業及通報程序悉依本公司「重大偶發事件通報處理辦法」、「個人資料檔案安全維護辦法」及「資通安全通報應變作業要點」辦理。

第六條 實施範圍

一、 資訊安全政策訂定。

二、 資通安全權責分工。

三、 人員管理及資通安全教育訓練。

四、 電腦系統安全管理。

五、 網路安全管理。

六、 系統存取管制。

七、 系統發展及維護安全管理。

八、　資通資產安全管理。

九、　實體及環境安全管理。

十、　業務永續運作計劃管理。

十一、資通安全查核。

第七條 實施內容

一、各項資通安全管理規定必須遵守政府相關法規（如：「建立證券商資通安全檢查機制」、「資通安全管理法」、「個人資料保護法」等）之規定。

二、由資訊服務部負責資通安全制度之建立及推動事宜。

三、定期實施資通安全教育訓練、宣導資訊安全政策及相關實施規定。

四、建立資通硬體設施及軟體之管理機制，以統籌分配、運用資源。

五、建置新資通系統前，應將資通安全納入考量因素，防範發生危害系統安全之情況。

六、建立電腦機房實體及環境安全防護措施，並定期實施相關保養。

七、明確規範資通系統及網路服務之使用權限，防止未經授權之存取動作。

八、訂定資通安全之業務持續運作計畫並實際演練，確保業務持續運作。

九、所有人員負有維持資通安全之責任，且應遵守相關之資通安全管理規定。

第八條 實施與修正

本政策每年應至少評估 1 次，以反映國家及客戶各項安全政策、法令、技術及業務之最新狀況，確保安全實務作業之可行性及有效性。

第九條 其他

本政策經董事會通過後實施，修正時亦同。