彰　化　銀　行

CHANG HWA COMMERCIAL BANK LTD.

資訊安全政策

Information Security Policy

V7.1

版本	修訂日	修訂者	核准日期	核准者	備註
V1.0	2004/05	資訊處	2004/05	總經理	
V2.0	2005/01	資訊處	2005/01	總經理	
V3.0	2006/01	資訊處	2006/01	總經理	
V3.1	2006/04	資訊處	2006/04	總經理	
V3.2	2006/12	資訊處	2006/12	總經理	
V4.0	2008/12	資訊處	2008/12	總經理	
V5.0	2009/12	資訊處	2009/12/29	第 22 屆第 8 次董事會	
V6.0	2013/05	資訊處	2013/05/14	第 23 屆第 20 次董事會	
V7.0	2018/01	資訊處	2018/01/19	第 25 屆第 8 次董事會	
V7.1	2018/09	資訊安全中心	2018/09/28	第 25 屆第 16 次董事會	

目　　錄

第一條 (宗旨)

彰化商業銀行股份有限公司(以下簡稱本行)為強化資訊安全管理、確保資訊的機密性、完整性與可用性、資訊設備（包括電腦軟、硬體及週邊設施）與網路系統之可靠性以及本行全體同仁對資訊安全之認知，並確保上述資源免受任何因素之干擾、破壞、入侵或任何不利之行為與企圖，特訂定本政策。

第二條 (參考依據)

一、個人資料保護法。

二、ISO/IEC 27001:2013 Information technology- Security techniques- Information Security Management System- Requirements。

第三條 (目標)

資訊安全之目標係為確保本行資訊的合法授權存取，於可能遭受內、外部威脅時，亦能提供完整、可靠之資訊系統運作，保證業務流程正常運行；於事故發生時，作迅速必要之應變處置，以降低該事故可能帶來之損害。

第四條 (範圍)

資訊安全政策之範圍，涵蓋本行所有資訊軟、硬體及週邊設施，有關單位及人員應就下列事項訂定相關管理規範以實施資安整體防護計畫，為實現本行營運的目標提供支持。

一、資訊安全權責分工。

二、人力安全管理。

三、電腦系統安全管理。

四、網路安全管理。

五、系統存取管理。

六、系統購置、開發及維護管理。

七、資訊資產安全管理。

八、資料保密管理。

九、實體及環境安全管理。

十、協力廠商與第三方供應廠商資訊安全管理。

十一、資訊安全風險評估管理。

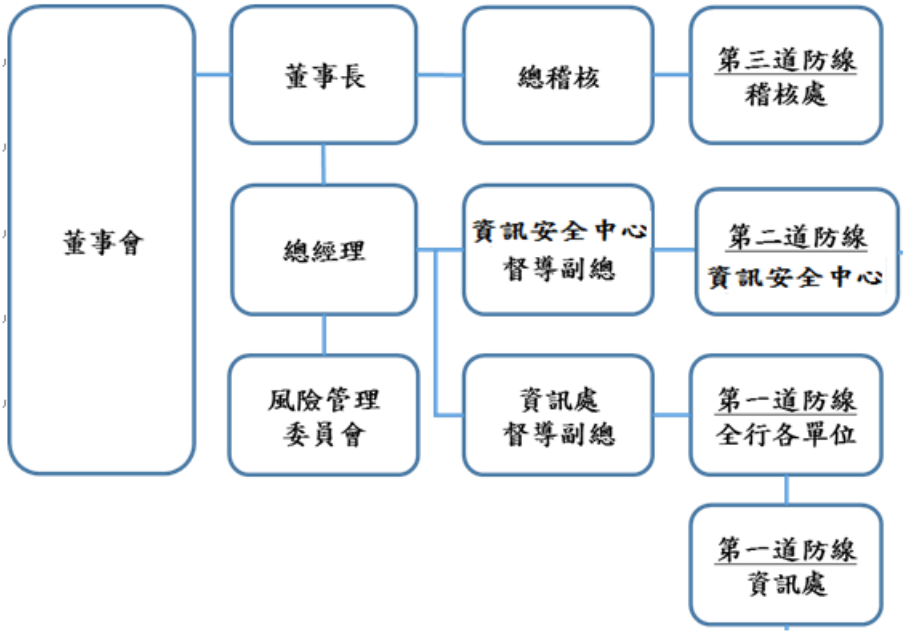
十二、資訊安全稽核管理。

十三、資訊安全教育訓練。

十四、其他資訊安全管理事宜。

第五條 (資訊安全組織架構)

為有效推行資訊安全工作，本行採行資訊安全三道防線之管理架構，第一道防線由全行各單位、資訊處負責執行資訊安全作業、第二道防線由資訊安全中心負責監控管理資訊安全政策之執行情形暨其衍生之資安風險，規劃、監控及執行資訊安全管理作業，第三道防線為稽核處檢查作業。



第六條 (權責分工)

本行為確保資訊安全管理能有效運作與實行，明訂相關組織權責分工，以推動及維持資訊安全各類執行、管理與查核等工作之進行，並應依下列分項原則，配賦適當之人員：

一、 資訊處主要職責在於推動資訊處管理制度、資訊安全系統監控處理及追蹤、執行法令法規要求之檢測及演練作業、資訊風險相關事件之通報及報告資料之回覆、資訊處資訊安全作業之覆核。

二、 資訊安全中心主要職責在於制定資訊安全相關政策、制定資訊安全風險評估準則、研擬資訊安全工具導入、執行資安檢測作業、規劃法令法規要求之檢測及演練作業、管理全行資訊安全作業相關程序及規範、管理全行資訊安全辦理情形、辦理資訊安全宣導教育訓練等。彙總全行資訊安全通報事件並評估後續改善情形、定期檢討報告資訊安全風險指標、定期報告全行資訊安全異常事件及改善情形、定期報告資訊安全風險評估結果、定期報告政策/準則/規範修訂之情形、定期報告資訊安全檢測/演練辦理情形等。

三、 稽核處主要職責在於辦理資訊安全查核作業。

第七條 (資訊安全專責主管)

本行由資訊安全中心主任擔任資訊安全專責主管，必須具備資訊安全相關背景，其功能性職責為負責監督和落實資訊安全政策與協調及推動資訊安全管理作業，並每年向董事會報告資訊安全整體執行管理情形。

第八條 (海外分支機構)

本行之海外分支機構除依循本行資訊安全政策、業務處理程序資訊篇及相關函文規定外，應依海外當地法令法規和監管要求制訂符合當地標準之資訊安全相關規範，二者最低要求不同時，應選擇較高標準者作為遵循之依據，並呈總行資訊安全中心審核後，提請總行風險管理委員會核備。

第九條 (政策之宣導)

本行應經由政策宣導、專題演講、教育訓練或電子媒體等方式，將資訊安全政策傳達至所有同仁與配合本行業務之資訊服務廠商，以期清楚認知本行資訊安全基準並確實遵循。

第十條 (資安事件通報)

各單位如發生資安事件，應即時依本行「資安事件通報管理施行細則」辦理。屬重大偶發事件時，應依本行業務永續運作計畫第二章第七條「重大偶發事件之通報」規定辦理。

又發生重大緊急事件時，應由資訊安全中心立即會同資訊處，分別報告其督導副總，立即採取適當應變措施，以降低該事故之損害，並確保業務持續營運。

第十一條 (違反資訊安全規定之處理程序)

本行全體同仁均須遵循資訊安全政策、資訊篇作業程序及相關函文規定，若有違反者，經查屬實，將斟酌情節處理，如：教育訓練、報告檢討、送人評會議處等方式處理。

第十二條 (政策之補遺)

本行之資訊安全政策若有未盡事宜，仍應依循資訊安全管理之精神與原則，確保本行資訊資產之機密性、完整性及可用性。

第十三條 (政策之例外豁免)

對於因法律規定、技術能力或成本效益之考量，需要例外管理之控制措施，必須經過申請、評估與核准程序，確定可否豁免於資訊安全政策外，以保持資訊安全管理機制之彈性與完整性，並經由風險管理委員會討論後提報常務董事會。

第十四條 (政策之施行與修正)

本政策應定期審視檢討。

本政策經 董事會核定後施行，修正時亦同。