彰　化　銀　行

CHANG HWA COMMERCIAL BANK LTD.

資訊安全政策

Information Security Policy

V8.5

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	
V8.0	2020/05	資訊安全中心	2020/05/07	第 25 屆第 37 次董事會	
V8.1	2021/07	資訊安全中心	2021/07/22	第 26 屆第 15 次董事會	
V8.2	2022/03	資訊安全處	2022/03/29	第 26 屆第 24 次董事會	
V8.3	2023/05	資訊安全處	2023/06/07	第 26 屆第 40 次董事會	
V8.4	2025/02	資訊安全處	2025/03/20	第 27 屆第 24 次董事會	
V8.5	2026/05	資訊安全處	2026/09/24	第 28 屆第 5 次董事會	

目　　錄

第一條　(宗旨).....1
第二條　(遵循依據).....1
第三條　(目標).....1
第四條　(範圍).....1
第五條　(資訊安全組織架構).....2
第六條　(權責分工).....3
第七條　(資訊安全長).....3
第八條　(資訊安全專責主管).....3
第九條　(海外分支機構).....4
第十條　(政策之宣導).....4
第十一條　(資安事件通報).....4
第十二條　(違反資訊安全規定之處理程序).....4
第十三條　(政策之補遺).....4
第十四條　(政策之施行與修正).....5

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 (遵循依據)

一、 個人資料保護法。

二、 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - 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。本行持續投入資訊安全防護系統所需之資源，以達成資訊安全目標。

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、 人員管理及資訊安全教育訓練。

三、 電腦系統安全管理。

四、 網路安全管理。

五、 系統存取管理。

六、 系統建置、開發及維護管理。

七、 資訊資產安全管理。

八、 資料保護管理。

九、 實體及環境安全管理。

十、 供應商及第三方資訊安全要求與管理。

十一、 資訊安全風險評估管理。

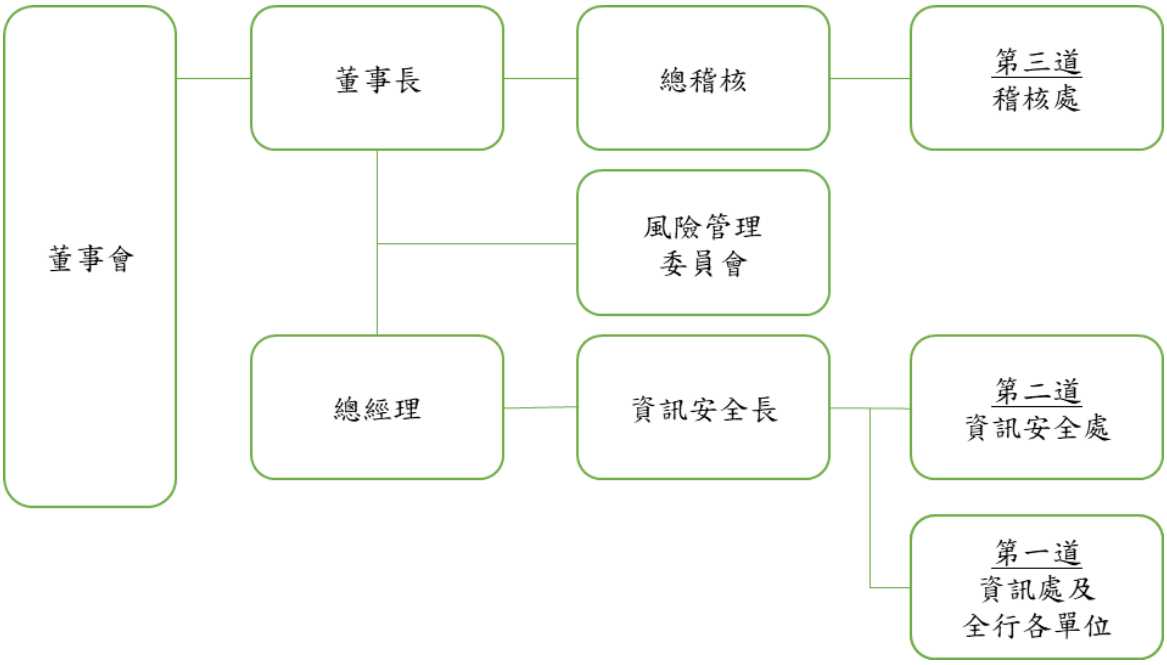
十二、 資訊安全稽核管理。

十三、 資訊安全威脅監控及回應。

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模型之管理架構，第一道由全行各單位、資訊處負責執行資訊安全作業，第二道由資訊安全處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，第三道為稽核處檢查作業。



圖一、資訊安全組織架構

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、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、 資訊安全處主要職責包括：

(一)負責資訊安全制度之規劃、管理及執行，以控管資訊安全風險。

(二)督導各單位落實資訊安全制度，並確保資通系統、服務及資訊之機密性、完整性與可用性。

(三)建立資通安全防護、資通安全情資之評估因應與資通安全事件通報及應變相關機制。

(四)每年應將前一年度資訊安全整體執行情形納入內部控制制度執行情形評估。

(五)辦理資訊安全教育訓練相關事宜。

三、 稽核處主要職責在於辦理資訊安全查核作業。

第七條 (資訊安全長)

本行由資訊安全長綜理資訊安全政策推動與資源調度事務，且每年應向董事會報告前一年度資訊安全整體執行情形，並及時報告重大資安問題。

第八條 (資訊安全專責主管)

本行由資訊安全處處長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。

第九條 (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，並呈總行資訊安全處審核後，提請總行風險管理委員會核備。

第十條 (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。

第十一條　(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「彰化銀行重大偶發事件處理程序」規定辦理。

倘若發生重大緊急事件時，應由資訊安全處與資訊處，分別報告資訊安全長及資訊處督導副總，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。

第十二條　(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、業務處理程序資訊篇及相關函文規定，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。

第十三條　(政策之補遺)

本行之資訊安全政策若有未盡事宜，仍應依循主管機關法令及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。

第十四條　(政策之施行與修正)

本政策應每年至少評估一次，或於發生重大變動時重新評估，以符合相關法令、組織及業務等之最新發展現況，確保資訊安全實務作業之有效性。

本政策經董事會核定後施行，修正時亦同。