王道商業銀行資訊安全政策

2025.6.23 第九屆第 19 次董事會核准後施行

第一條　依據及目的

依中華民國銀行商業同業公會全國聯合會金融機構資通安全防護基準第三條之規定，本行為確保資訊資產之機密性、完整性、可用性及適法性，並避免遭受內、外部蓄意或意外之威脅，爰衡酌本行之業務需求，訂定本政策。

第二條　適用範圍

本行全體人員(包含所有員工、約聘人員、派遣人員)、第三方廠商等，皆應遵守本政策。

第三條　名詞定義

一、資訊資產（Information assets）：凡與資訊處理相關之資產皆屬之，包括硬體、軟體、資料、文件及人員等，皆視為資訊資產。

二、機密性（Confidentiality）：確保只有獲得授權的使用者，才得以存取資訊；

三、完整性（Integrity）：保障資訊與處理方法的正確與完整；

四、可用性（Availability）：確保獲得授權的使用者於有需求時，能適時存取資訊及相關資產。

第四條　資訊安全目標

本行之資訊安全目標如下：

一、　確保本行資訊資產之機密性，落實資料存取控制，資訊需經授權人員方可存取。

二、　確保本行資訊資產之完整性，避免未經授權之修改。

三、　確保本行資訊作業之持續運作。

四、　確保本行資訊作業均符合相關法令規定要求。

第五條　資訊安全控制措施

本行之資訊安全控制措施如下：

一、　管理階層應承諾維護資訊安全，持續改善資訊安全管理制度以因應資安風險，減少資訊安全事故之發生，以保障客戶之權益。

二、　本行全體人員皆有責任及義務保護其擁有、保管或使用之資訊資產。

三、　工作分派應考量職能分工，職務責任範圍應予區分，以避免資訊或服務遭未經授權修改或誤用。

四、　對於與本行有業務往來之第三方廠商依合約簽定存取本行資訊資產之需求時，本行應對廠商進行必要之審核、宣導本行之資訊安全相關政策，廠商亦須遵循本政策及中華民國銀行商業同業公會全國聯合會「金融機構資通系統與服務供應鏈風險管理規範」，該等人員並負有保護其所存取、保管或使用本行資訊資產之責任。

五、　確保工作區域場所之安全，以防範資訊資產遭竊取或毀損。

六、　落實通訊安全管理。

七、　因應作業需求或其他因素(如：重大疫情)須與本行進行遠端連線者，原則上應使用虛擬桌面基礎架構(VDI)或虛擬私有網路(VPN)，賦予最小權限，並遵循本行相關資安規定。

八、　本行應積極監測網路安全風險(cybersecurity)及因應資訊安全威脅，隨時注意是否有發生資訊安全事件、安全弱點及違反安全政策之虞等情事，並依程序進行資訊安全事件通報、迅速回應及實施緩解措施。當發生資安事件時，應即時向受影響的利害關係人揭露該資安事件狀況，並且說明後續因應作為及未來防範相關風險之措施。

九、　應採用行動裝置安全措施，以管理使用行動裝置所導致之風險。

十、　成立資訊安全管理組織，以維護資訊安全管理制度之運作，鑑別資訊安全管理制度之內、外部議題及利害相關團體對本行之資訊安全要求與期望，定期

進行資訊資產分類、風險評鑑以及資訊安全指標作業，遵循內外部相關法令規定，建立應有之管控程序及適時更新作業，並定期執行資訊安全查核作業。

第六條　年度審查

本政策每年至少審查一次，以符合相關法令規定及資訊業務最新發展現況，並於必要時修正之。

第七條　附則

一、　本政策有關作業要點由資訊單位另訂並經總經理通過後實施，修改時亦同。

二、　本政策呈董事會核定後實施，其修訂時亦同。

修訂歷程：

●	核定日期	制/修訂說明	權責單位	核准層級
1	2018/10/30		資訊安全部	第七屆第 13 次董事會核准後施行
2	2019/04/26		資訊安全部	第七屆第 17 次董事會核准後施行
3	2022/03/16		資訊安全部	第八屆第 14 次董事會核准後施行
4	2024/01/31		資訊安全部	第九屆第 6 次董事會核准後施行
5	2025/6/23	1. 配合規章制定作業原則修訂，新增政策之依據。 2. 配合永續發展及實務作業修訂。	資訊安全部	第九屆第 19 次董事會核准後施行