【ChaiBo App】快速登入暨行動御守 2.0 安控交易服務約定事項

申請人茲向貴行申請快速登入暨行動御守 2.0 安控交易服務(下合稱本服務)，並同意遵守下列約定事項：

一、名詞定義

(一) 行動裝置：係指包含但不限於智慧手機、平板電腦等具通訊及連網功能之設備。

(二) 綁定行動裝置：係指申請人於行動裝置安裝貴行指定之應用程式，並按指示輸入相關資訊以完成綁定程序。

(三) 行動御守 2.0 安控機制：係指申請人於完成綁定程序之行動裝置，透過與貴行約定且設定完妥之安控機制(例如圖形鎖、指紋、臉部等申請人擁有之生物特徵、固定數字密碼或離線交易密碼等)。

(四) 快速登入：係指申請人於完成綁定程序之行動裝置，以與貴行約定且設定完妥之安全機制(例如圖形鎖、指紋、臉部等申請人擁有之生物特徵等)登入貴行允許之應用程式，無須依照一般登入方式(即輸身分證字號、使用者代碼及使用者密碼)進行登入。

(五) 離線交易密碼：申請人自行設定 6 至 12 位數字之離線交易密碼，作為已綁定之行動裝置離線時交易之驗證。

二、綁定行動裝置

(一) 申請人應利用貴行應用程式依指示輸入向貴行(臨櫃)申請行動御守 2.0 安控交易服務所取得之驗證碼、透過 ATM/網路銀行設定之驗證碼或線上透過 SIM 卡認證等方式，完成綁定程序，以確認行動裝置為申請人所持有。同一行動裝置不得由兩名以上申請人申請綁定，且申請人至多僅得申請綁定一台行動裝置。

(二) 申請人同意必須透過完成綁定程序之行動裝置使用本服務。

三、行動御守 2.0 安控機制交易服務

(一) 存款帳戶交易服務

1.申請人得使用行動御守 2.0 安控機制，即時自申請人指定存款帳戶扣款進行包括非約定帳戶之轉帳、繳費稅及消費扣款等交易。

2.交易限額如下：

(1)非約定帳戶轉帳：每筆等值新臺幣 5 萬元、每日等值新臺幣 10 萬元及每月等值新臺幣 20 萬元。

(2)繳費：每筆等值新臺幣 200 萬元及每日等值新臺幣 300 萬元。

(3) 繳稅：每筆等值新臺幣 200 萬元及每日帳戶可用餘額。

(4) 消費扣款：

一維條碼(Bar Code)及二維條碼(QR Code)：每筆等值新臺幣 5 萬元、每日等值新臺幣 10 萬元、每月等值新臺幣 20 萬元。

(5)非約定帳戶轉帳及消費扣款每日等值新臺幣 10 萬元及每月等值新臺幣 20 萬元應合併計算。

(6)掃碼提款：每筆等值新臺幣 2 萬元、每日等值新臺幣 2 萬元及每月等值新臺幣 2 萬元。

(二) 小額快速交易功能

1.申請人同意如開啟【彰銀錢包】之小額快速交易功能(信用卡交易不適用)時，視為申請人在每筆交易金額在等值新臺幣 3 千元(含)以下，同意貴行無須再以行動御守 2.0 安控機制進行驗證，即得逕自指定存款帳戶即時扣款完成交易。

2.小額快速交易之交易筆數限制為每日 5 筆。

(三) 信用卡交易

1.申請人如持有貴行發行之信用卡，可利用【彰銀錢包】掃碼或付款碼之功能，經由行動御守 2.0 安控機制進行驗證後，以申請人指定之信用卡進行繳稅費或消費交易，申請人同意以【彰銀錢包】所為之信用卡交易行為等同實體信用卡所為，且信用額度應與連結之實體信用卡共用。

2.申請人利用【彰銀錢包】進行信用卡交易，仍應繼續遵守「彰化銀行信用卡約定條款」。

四、停用、恢復及註銷

(一) 申請人以圖形鎖進行快速登入貴行應用程式或以圖形鎖進行行動御守 2.0 安控機制交易之錯誤(或失敗)次數分開計算。使用圖形鎖之錯誤次數連續達 3 次時，快速登入功能將無法使用，改為一般登入方式。

(二) 行動御守 2.0 安控機制，驗證錯誤次數達 3 次時，申請人得依指示重新輸入臨櫃申請之新驗證碼、透過 ATM/網路銀行設定之驗證碼或線上透過 SIM 卡等認證方式，重新完成綁定程序，以恢復本服務之使用。

(三) 行動御守 2.0 安控機制或快速登入，原為不啟用，可透過使用者密碼驗證後啟用。

(四) 申請人若不再使用本服務時，可臨櫃、經由個人網路銀行或貴行客服中心申請註銷。

五、其他

(一) SIM 卡認證注意事項如下

1. 申請人進行認證 SIM 卡之手機號碼需為申請人留存於貴行之手機號碼。
2. 手機號碼認證服務支援之電信公司為：中華電話、台灣大哥大及遠傳(含 ibon mobile)。
3. 行動裝置如使用 VPN、防火牆軟體，申請人應關閉後再進行 SIM 卡認證。
4. 若行動裝置為雙卡機者，申請人應確保用於行動網路連線的 SIM 卡之手機號碼為留有於貴行之手機號碼。
5. SIM 卡認證方式，設有次數上限。
6. 申請人如在國外擬進行 SIM 卡認證，應開啟國際漫遊服務，且因認證過程會確認申請人 SIM 卡之上網 IP 位置，可能因 IP 位置在國外而認證失

敗，如 SIM 卡認證失敗，申請人應改以驗證碼的方式進行綁定行動裝置。

(二) 申請人應妥善保管已綁定之行動裝置，且不得讓第三人知悉申請人所設定之行動御守 2.0 安控機制之資訊(包括圖形鎖或指紋、臉部等申請人擁有之生物特徵或固定數字密碼等)，亦不得以任何方式讓與或轉借他人使用。

(三) 申請人應親自完成行動裝置綁定程序及行動御守 2.0 交易安控及密碼之設定，申請人同意經由該行動裝置登入貴行應用程式或所為之交易，均視為申請人本人所為之有效指示，申請人絕無異議。

(四) 申請人不得任意破解(越獄及 Root)行動裝置、與他人共用行動裝置(或儲存他人之指紋/臉部等生物特徵)並應慎防駭客攻擊以確保帳戶安全，如因第三人冒用或盜用所致損害，申請人應自行負責，倘致貴行受有損害時，申請人亦應負賠償之責；惟申請人能舉證本服務之冒用或盜用係因貴行對資訊系統之控管未盡善良管理人注意義務所致者，則由貴行負賠償之責。

(五) 申請人發現第三人冒用或盜用使用者持有行動裝置或知悉行動御守 2.0 安控機制等資料時，應立即通知貴行停止本服務並採取防範措施。

(六) 貴行有權因風險考量暫時或永久停止有安全疑慮之特定機型之行動裝置使用生物特徵辨識驗證功能。

(七) 為防制洗錢及打擊資恐之目的，申請人同意貴行得依「洗錢防制法」、「資恐防制法」、「金融機構防制洗錢辦法」、「存款帳戶及其疑似不法或顯屬異常交易管理辦法」、「金融機構辦理國內匯款作業確認客戶身分原則」、「銀行業及其他經金融監督管理委員會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法」、銀行等各業別所屬同業公會防制洗錢及打擊資恐注意事項範本等涉及防制洗錢及打擊資恐之相關法規命令規定、「銀行業辦理外匯業務作業規範」、「銀行業輔導客戶申報外匯收支或交易應注意事項」等有關規定及(或)其嗣後修訂施行之法規命令，確認及持續審查並要求提供(提供時點包括但不限於嗣後加開帳戶、新增業務往來關係時、定期審查時點、身分與背景資訊有重大變動時等)申請人與受款人、受款銀行之身分及資料(包括但不限於最新身分證明文件、公司登記文件等)、保存及向有關機關申報或報送相關交易憑證及資料。

(八) 「申請人同意，貴行如因業務關係依美國洗錢防制法(Anti-Money Laundry Act of 2020，AMLA)第 6308 條規定，經美國財政部、司法部、法院、其他監理機關或司法機關要求提供申請人及/或關係人（包括但不限於申請人之負責人、實質受益人、高階管理人員、代理人、代表人、被授權人或交易相對人等）之業務往來相關資料，貴行得配合進行蒐集、處理、利用與國際傳輸，毋須另行通知申請人及/或關係人。申請人並同意，貴行依前述約定所採取之行為，對申請人及/或關係人不負任何損害賠償/損失補償責任。」

(九) 申請人如有下列情形之一時，貴行得拒絕與申請人為新增業務往來、暫時停止申請人之交易、暫時停止或終止貴行與申請人之個人網路銀行業務關係、逕行終止個人網路銀行、申報可疑交易或採行其他必要措施：

1.申請人或其實質受益人、高階管理人、關聯人(如法定代理人、代理人、被授權人)、交易對象，為資恐防制法指定制裁之個人、法人或團體，以及外國政府或國際組織認定或追查之恐怖分子或團體時。

2.不配合審視(包括但不限於電話、信函或實地查核作業)、拒絕或拖延提供立約人、其實質受益人(包括但不限於股權結構、高階管理人員與關聯人等資料)客戶或對其有控制權之人等資訊，或對交易之性質與目的或資金來源不願配合說明等情事。

(十) 申請人如有下列情形之一時，貴行得拒絕與申請人為業務往來、暫時停止申請人之交易、暫時停止或終止貴行與申請人之業務關係、逕行終止本服務或採行其他必要措施(包括但不限於要求申請人再次進行確認身分程序)：

1.申請人登入貴行應用程式或交易出現異常情形。

2.有相當事證足認申請人利用貴行應用程式從事詐欺、洗錢等不法行為或疑似該等不法行為時。

(十一) 申請人同意與貴行間使用本服務得以電子訊息為表示方式，其效力與書面文件相同。電子訊息係指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用。

(十二) 本服務約定事項如有修改或增刪時，貴行得於營業處所或網站(www.bankchb.com)公告，申請人於 7 日內不為異議者，視為承認該修改或增刪約定事項。

(十三) 除貴行及申請人另有約定外，本服務約定事項如有其他未盡事宜，悉依申請人另行簽訂之「存款相關服務性業務約定條款(個人戶)」/「數位存款帳戶約定條款」及中華民國法令規定辦理。