恒生銀行
HANG SENG BANK

# 電子管道安全性措施

本文件將說明電子銀行業務系統 (下稱「**電子管道**」) 的安全性措施 (恒生銀行或HSBC集團可能會不定期修訂或更新)，適用範圍為恒生銀行或HSBC集團旗下任何成員(下稱「**銀行**」) 向客戶 (下稱「**客戶**」) 提供的任何電子銀行業務系統。

## 銀行安全性措施

1. 銀行應採取相關措施，拒絕未經授權的外部人士存取其網際網路服務營運的環境。
2. 銀行應確保自家系統受到嚴格控管，包括設立營運持續方案。
3. 根據銀行的安全性措施，由客戶授權存取恒生 HSBCnet 電子管道的使用者 (下稱「使用者」) 若長達 6 個月未有登入恒生 HSBCnet，可能會自動被系統暫停使用。如有恒生 HSBCnet 之設定檔在長達 18 個月的時間中沒有任何使用者戶存取，該恒生 HSBCnet 設定檔可能也會被暫停使用。
4. 如果使用生物特徵驗證方式 ( 如指紋掃描或臉部辨識 ) 從行動裝置存取電子管道，銀行及其提供應用程式至行動裝置的關聯 HSBC 實體，保留任何時間視需要移除生物特徵驗證功能的權力，若裝置有安全性相關疑慮則不另行通知。在正常情況下，仍然可以使用其他現有方法透過行動裝置進行驗證。

## 客戶安全性措施

1. 客戶只能透過銀行指定的驗證方式存取電子管道。
2. 客戶應確保所有使用者均能妥善保管其安全性認證 ( 密碼、提示問題的答案、安全性答案、安全裝置 PIN、行動裝置密碼 / PIN 或任何需要存取電子管道的安全性認證 (如適用) )，並維持此類資訊的機密性，同時不幫助對這些認證進行任何未經授權的使用。
   特別是客戶不得與任何第三方分享任何安全性認證或存取電子管道，但已獲得客戶授權且受到規範之第三方服務供應商則不在此限。
3. 客戶有責任謹慎挑選使用者，須考量到這些使用者將能存取多種功能，包括向賬戶或其他服務指派權限，以及傳送與這些賬戶或服務有關的指示。
4. 若任何安全裝置遺失或遭竊，客戶應立即通知銀行。
5. 客戶應：
   (a) 在懷疑任何使用者的認證透過任何方式遭到部分或完全盜用時，立即採取適當動作保護該使用者的設定檔；
   (b) 在懷疑任何使用者的認證遭盜用時，審查其賬戶和使用者設定檔的近期活動，並在有任何異常情況時，立即通知銀行；以及
   (c) 定期審查其賬戶和使用者設定檔的活動，藉此確保沒有違規行為，並在有任何異常情況時，立即通報銀行。
6. 如有任何使用者離開客戶的機構，客戶應立即從電子管道設定檔中移除該使用者。若對使用者的行為或權限有任何疑慮，客戶應立即暫停該使用者對電子管道的使用。客戶應確保安全性認證或裝置僅由指派的特定個人使用者使用，但已獲得客戶授權且受到規範之第三方服務供應商則不在此限。
7. 客戶應確保其使用者在銀行提出要求時，皆提供正確，詳實且未經省略的詳細資料。客戶應進一步確保其使用者會定期檢視此類資訊，並在有所變更時更新詳細資料，且任何時候皆只維護一個使用者名稱或一組安全性認證。
8. 客戶若得知銀行已寄送安全裝置，卻未收到寄送的包裹，則應在寄送後的七天內通知銀行。
9. 若經銀行要求，客戶應立即將任何安全裝置歸還給銀行。
10. 客戶應定期採用及審查其內部安全性措施，藉此確保所有保護措施保持在最新狀態，並符合法規及產業的最佳實務指示。這包括但不限於惡意軟體防護、網絡限制、實體存取限制，遠端存取限制、電腦安全性設定、不當使用情況的監控、可接受的網路瀏覽器與電子郵件使用方式(包括如何避免收取惡意軟體 ) 的指引。
11. 客戶應設立相關流程，避免使用者遭受到社會工程攻擊或聽從詐騙通訊的指示行動。這是為了防止企業電子郵件遭盜用和其他類似的攻擊手法，避免詐騙者冒充為電子管道之授權使用者已知的對象，並寄送電子郵件給授權使用者，企圖變更收款對象的地址或銀行賬號。此類流程應包括如使用者收到看似來自已知寄件者(包括但不限於高級管理階層、供應商和廠商 ) 的通訊內容時，如何確保獨立驗證 ( 透過電子郵件以外的方式 ) 此類通訊內容的真實性。
12. 若使用者透過行動裝置存取任何電子管道，客戶應要求該使用者：
    (a) 登入任何電子管道後，切勿讓行動裝置處於無人看管的情況下；
    (b) 存取完任何電子管道後，按「登出」按鈕；
    (c) 啟用行動裝置的自動密碼鎖定功能；
    (d) 不與他人共用用於存取電子管道的行動裝置；
    (e) 為裝置中唯一註冊了生物驗證 ( 臉部辨識、指紋、聲音、視網膜 ) 的人；
    (f) 於發生第 15 條假設情境之場合，採取行動以取消註冊不得再度用於驗證的裝置；以及
    (g) 不使用任何已越獄，取得根權限或遭破解的行動裝置存取電子管道。
13. 客戶瞭解並同意，其電子管道若因任何原因遭停用，該電子管理後續的任何重新啟用作業，都會將所有權限、限制、使用者存取權以及對相同賬戶和服務的存取權，恢復至停用前的原始狀態。
14. 客戶應瞭解，使用行動裝置存取電子管理的使用者可以透過該裝置執行廣泛的活動。這包括使用行動裝置 ( 如代替安全裝置 ) 驗證經由桌上型電腦在另一電子管道執行的活動。
15. 當使用者經由某些行動裝置上可用的生物特徵驗證方式存取電子管道時 ( 如指紋掃描或臉部辨識 )，客戶瞭解此種驗證方式依舊存在遭破解或允許未經授權的存取的風險 ( 例如親近的家庭成員涉入 )。