電子渠道安全措施

本文件闡述了滙豐集團成員（以下簡稱“業務關係行”）向其客戶（以下簡稱“業務關係所有人”）提供任何電子銀行系統（以下簡稱“電子渠道”）的安全措施（經滙豐集團不時的修訂或更新）。

1. 業務關係行安全措施

1.1. 業務關係行應採取措施不讓未經授權的外部人士對其互聯網服務運行環境進行訪問。

1.2. 業務關係行應確保其係統受到嚴格控制，包括制定業務連續性計劃。

1.3. 作為業務關係行安全措施的一部分，由業務關係所有人授權可訪問滙豐財資網電子渠道的用戶（“用戶”），如在 6 個月內未登錄滙豐財資網，其登錄權限將自動暫停生效。如果某滙豐財資網客戶資料在 18 個月內未被任何用戶訪問， 則該客戶資料也會被暫停訪問。

1.4. 如果使用生物識別認證方法（例如指紋掃描或面部識別）從移動設備訪問電子渠道，則向移動設備提供應用程序的業務關係行和相關滙豐實體保留在必要情況下（如出現與設備安全相關的問題）無需通知即可隨時刪除生物識別認證功能的權利。在正常情況下，使用其他現有方法通過移動設備進行身份驗證仍可行。

2. 業務關係所有人安全措施

2.1. 業務關係所有人應只採用業務關係行規定的認證方法訪問電子渠道。

2.2. 業務關係所有人應確保所有用戶始終保證安全證書（密碼、提示答案、安全問題答案、安全設備 PIN 碼、移動設備密碼/PIN 或訪問電子渠道所需的任何其他安全證書（如果適用））安全且處於保密狀態，且不支持在未經授權的情況下使用這些證書。尤其是，業務關係所有人不得與經其適當授權的受監管的第三方服務提供商以外的任何第三方分享安全證書或電子渠道的訪問權。

2.3. 業務關係所有人應謹慎選擇其用戶，因該等用戶有權進行廣泛的活動，包括賦予有關賬戶或其它服務的授權並代表業務關係所有人和/或開戶人發出指令。

2.4. 當任何安全設備丟失或被盜時，業務關係所有人應立即通知業務關係行。

2.5. 業務關係所有人應：

(a) 在懷疑用戶證書已經以任何方式全部或部分受損時， 立即採取適當行動來保護該用戶的個人資料；

(b) 在懷疑用戶證書已經被受損時，對其賬戶上的近期活動及用戶資料進行審核，並且立即將發現的任何差異通知業務關係行； 且

滙豐

由香港上海滙豐銀行有限公司（澳門分行）刊發

(c) 定期審核其賬戶以及用戶的資料活動及權限，以確保不存在任何異常，並且及時向業務關係行滙報發現的任何差異。

2.6 如果任何用戶離開業務關係所有人的機構，業務關係所有人應立即禁止該用戶使用電子渠道。業務關係所有人如果對任何用戶的行為或其權限有任何疑慮，則應立即暫停該用戶的電子渠道使用權。除業務關係所有人適當授權的受監管的第三方服務提供商以外，業務關係所有人應確保安全憑據或安全設備僅被獲得該等憑據或設備的特定個人用戶使用。

2.7 關係所有人應確保每當其用戶被滙豐集團要求時提供正確的，全面的且未經縮寫的詳細信息。業務關係所有人應進一步確保其用戶定期審查此詳細信息且每當其詳細信息發生變化時更新其詳細信息並在任何時候不會持有多個用戶名或多套安全證書。

2.8 業務關係所有人應在業務關係行發出安全設備後七天之內，通知業務關係行其尚未收到發送的包裹，但前提是業務關係所有人收到了派件提示。

2.9 一旦業務關係行提出要求，業務關係所有人應立即將安全設備歸還業務關係行。

2.10 業務關係所有人應採取並定期審查內部安全措施，以確保保護措施及時且符合法規和行業最佳實踐指導。此等保護措施應當包括（但不限於）惡意軟件防護、網絡限制、物理訪問限制、遠程訪問限制、電腦安全設置、監控不當使用、關於如何選擇可接受的網頁瀏覽器和使用電子郵件（包括如何避免沾染惡意軟件）的指導。

2.11 業務關係所有人應有措施防止用戶陷入社交工程陷阱或根據欺詐指令行事。此項是為防止商業郵件欺詐或類似騙局，即行騙者發送郵件假扮為電子渠道的授權用戶所認識的某人，從而試圖修改接收款項的地址或銀行賬號。例如，該等措施應包括：若從看似認識的發送人（包括但不限於高級管理層、賣方或供應商）處收到通訊信息，應確保對該等通訊信息的真實性（以非電子郵件形式）進行獨立驗證。

2.12 當用戶通過移動設備訪問任何電子渠道時，業務關係所有人應要求該用戶：

(a) 不要在登錄到任何電子渠道之後，使移動設備處於無人看管狀態；

(b) 在用戶結束電子渠道訪問後，點擊`退出'按鈕；

(c) 啟用移動設備的自動密碼鎖功能；

(d) 不與他人共享用於訪問電子渠道的移動設備；

(e) 是唯一在設備上註冊生物識別（例如面部、指紋、語音、視網膜識別等）的人士；

(f) 根據第 15 條的規定，註銷不應再用作身份驗證的設備；以及

(g) 不通過已被破解、取得根權限或以其他方式被破壞的移動設備訪問電子渠道。

2.13 業務關係所有人確認並同意，如果其電子渠道由於任何原因被暫停使用，該電子渠道在被重新激活後，將自動恢復與暫停之前相同的原權限、限額、用戶訪問以及可訪問的賬戶和服務。

2.14 業務關係所有人應注意，通過移動設備訪問電子渠道的用戶可以使用設備開展各種活動。這包括利用移動設備（例如代替安全設備）對通過台式計算機執行的單獨電子渠道會話中開展的活動進行身份驗證。

2.15 如果用戶通過可在某些移動設備上使用的生物識別身份驗證方式（例如指紋掃描或面部識別）訪問電子渠道，則業務關係所有人承認此類認證方式仍然存在被破壞或允許未經授權人士（例如在涉及親密的家庭成員的情況）訪問的風險。