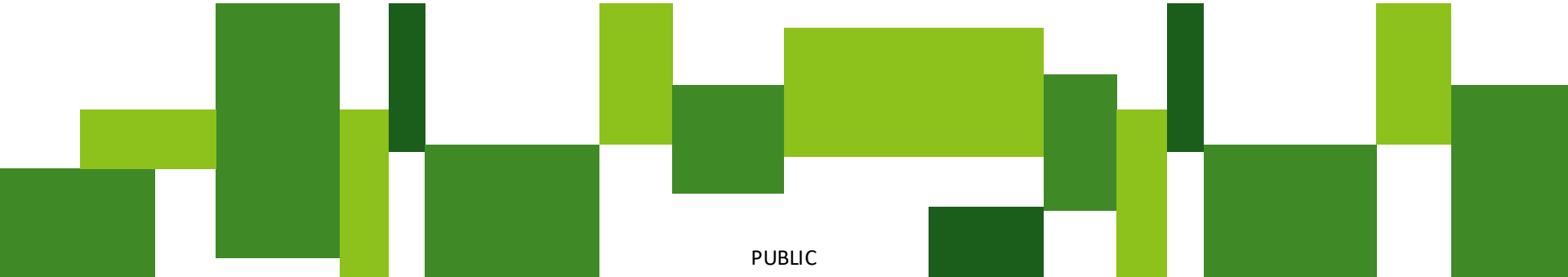
恒生銀行
HANG SENG BANK

恒生HSBCnet安全特點

2023



PUBLIC

恒生銀行的網上安全方針

本行旨在為客戶提供穩健、可靠且安全的線上業務環境。 我們設法透過採用「同類最佳」的技術、制定最佳實務資訊科技政策及程序的組合，並讓專業資源致力於實行及監督，以達成我們的目標。 我們採用業界標準解決方案，在客戶登入時驗證其身分，確保以安全可靠的方式傳輸客戶資料，並保護客戶資料的安全。我們擁有備分及應變計劃，可確保將不論因為任何原因而發生服務中斷狀況的機率降到最低。憑藉我們作為安全電子銀行業務系統提供者，擁有豐富經驗，我們還運營一個控制及支援結構，旨在確保銀行在提供網上銀行交易時，能因應所面臨的各種風險層面。

安全特點

- 穩健身份驗證流程
- 防止鍵盤記錄及阻斷服務攻擊
- 使用實體保安編碼器或流動保安編碼器產生的一次性密碼進行雙重驗證
- 採用「傳輸層安全性」(TLS) 加密技術保護客戶與恒生銀行之間的資料傳送
- 保護敏感資料傳送及儲存確保客戶資料機密性
- 採用業界標準的安全機制保護基礎建設
- 定期對系統安全進行獨立審查
- 涵蓋系統及安裝開發與管理的穩健且定期審查的資訊安全政策
- 全面的應急及後備安排
- 24/7 安全監控及中央事故管理團隊
- 行政及交易活動的審計追踪

恒生HSBCnet驗證

安全認證及雙重驗證

恒生HSBCnet旨在根據一系列認證，來驗證登入系統的使用者。每一種認證都經過設計，能對抗我們在網際網路上驗證身分時面臨的多種風險。恒生HSBCnet 會設法以多種方式驗證使用者的身分，每種方法都經過特別設計，會將被存取的服務或功能的相關風險，與適當的安全級別進行比對。這些方式包括傳統的使用者名稱及密碼，並使用「提示問題」的額外認證加以輔助，加強針對阻斷服務攻擊的保護，以及使用實體保安編碼器或流動保安編碼器產生的一次性密碼進行雙重身份驗證。

風險較高的服務及功能受到雙重身份驗證的保護（在以實體保安編碼器及流動保安編碼器登入級別的情況下）。雙重驗證是傳統密碼式安全性防護的加強版，因為它不僅基於閣下已知的資料（在本例中為使用者名稱及實體保安編碼器或流動保安編碼器的密碼），閣下亦必須擁有實際的工具（即已啟動流動保安編碼器的流動裝置或實體保安編碼器），以及閣下固有的東西（即已於流動裝置啟用的生物認證（Touch ID / Face ID / 指紋認證 – 如啟用）。因此，潛在的攻擊者必須取得第二個或第三個因素 (即實體保安編碼器或已啟動流動保安編碼器的流動裝置及其密碼或生物認證)，才能入侵使用者的帳戶，因此這種驗證方式可以消除因網際網路上分散所導致的諸多滲透風險。

未經授權的存取嘗試

若有人試圖存取閣下的恒生HSBCnet帳戶，卻無適當的認證，系統將會在數次不成功的嘗試後鎖定帳戶。但是，為了降低他人惡意鎖定閣下的恒生HSBCnet帳戶的風險，本行也實施了阻斷服務攻擊防護。目的是確保只知道使用者名稱的人士受到質疑時，無法藉由輸入錯誤數值而鎖定該使用者的帳戶。

使用TLS已加密的工作階段

在閣下輸入安全性敏感資料(例如：密碼)時，畫面上會遮蔽這些字元。當資料從客戶的瀏覽器傳送到恒生銀行時，系統會將傳送的資料加密(透過TLS，亦即「傳輸層安全性」)。抵達恒生銀行時，此資料會在資料庫內加密。即使恒生HSBCnet的系統管理員也無法存取這項資訊。

若有人取得我的認證且能存取系統，我要如何判斷是否發生過這種情況?

恒生HSBCnet應用程式內有客戶可以使用的工具，用以檢閱特定使用者執行過的活動。

- ❖ 當閣下登入時，閣下的主要登陸頁面會指出此帳戶上次登入的時間。
- ❖ 使用者帳戶執行的任何業務或管理活動，都能藉由「活動查詢」工具檢視。

資料傳輸安全

閣下與恒生HSBCnet之間的安全性詳細資料傳輸，以及所有線上管理或交易活動，均使用TLS通訊協議加密。

基本加密涉及從一方傳輸資料到另一方的過程。傳送方會將資料編碼後再傳送。接收方必須以正確的「解碼器」將資料解密後才能讀取及使用。加密的效果是以使用的密鑰的複雜程度來衡量的。密鑰越複雜，沒有正確解碼器的人破解程式碼的時間則越長。

TLS是一種業界標準協議，用於保護網絡瀏覽器與恒生銀行之間的互聯網通訊。恒生銀行目前支援TLS 1.2及以上版本。

資料機密與完整性

恒生銀行採用安全行業最佳實務來保護客戶或個人資料。註冊時，每個使用者都會看到銀行的資料隱私聲明，聲明中詳述我們為使用者提供的保障並尋求使用者的同意。此外，使用者的資訊不會被寫入磁碟，或儲存在與網際網絡連結的網路伺服器上。網路伺服器實際上與保留傳輸資料的後台資料庫是分開的。因此，我們不會在網絡伺服器上保存客戶交易資料。敏感資料，例如客戶密碼，則使用硬件安全模組儲存在加密資料庫中。

恒生HSBCnet功能特點

以下描述恒生 HSBCnet 內建的一些功能特性，讓閣下更輕鬆地控制系統的使用。

存取級別

恒生HSBCnet為客戶員工提供兩種存取級別。系統管理員可以執行(在雙重或單方控制下)一般管理工作，例如設定及授權使用者使用恒生HSBCnet 的工具，以及暫停或刪除使用者。

終端使用者無權存取管理功能。任一類型的使用者都能被分配交易功能，但系統有足夠彈性，因此可以完全隔離管理與交易功能。

使用者存取控制

存取控制工具允許閣下指定的恒生HSBCnet系統管理員決定個別使用者的存取權利及權限，以及帳戶級別檢視及付款授權限制。

閣下可以設定授權付款所需的使用者人數，以及不同付款金額的使用者級別組合。閣下可以建立一套系統，要求不同國家或總公司對超過特定金額的付款進行授權。這可完全控管存取及授權，同時提高付款處理效率。

雙重授權管控

恒生 HSBCnet 中的所有重大的管理及業務功能均能以雙重授權控制（一名使用者提交交易/請求；另一名則需要為其授權）。 然而，應用程式也為客戶提供靈活性，讓他們可以定義是否需要雙重授權）。但是，在正常操作情況下，我們強烈建議選擇雙重管控選項。

活動記錄工具（審計追踪）

主要管理及交易事件會由恒生HSBCnet記錄，並提供使用者透過活動查詢記錄工具在線上檢視。我們會提供審計追踪，允許追溯內部控制及系統活動的財務審查。

逾時操作

恒生HSBCnet會強制執行閒置（無活動）的逾時操作。若操作時段在一段時間後維持無活動，操作時段會被終止，使用者必須重新登入應用程式。此外，使用者在操作時段期間檢視的頁面，在逾時後也不會儲存在瀏覽器中，讓其他使用者稍後可以存取這些頁面。

恒生HSBCnet安全性準則

閣下需為自己的系統，連接，以及提供給銀行的指示負責。閣下必須實施下列措施以保護自己，包括：

安全憑證

使用者必須隨時保管好自己的安全憑證（密碼，提示問題答案，實體保安編碼器或流動保安編碼器的密碼，或其他存取恒生HSBCnet所需的安全性憑證），並確保沒有未經授權使用或試圖入侵這些憑證的情況。 尤其是：

- 切勿寫下，記錄或向其他人泄露這些憑證;
- 立即銷毀任何來自銀行或其他方的憑證通知;
- 請勿使用容易猜到或推斷的安全憑證（例如：個人詳細資料，簡單的數字組合);
- 切勿在任何可自動保留憑證的軟件上記錄密碼，提示問題答案，安全性答案，或保安密碼(例如：電腦螢幕提示或使用者網際網路瀏覽器的「儲存密碼」功能);
- 確保使用者在登入恒生HSBCnet時並無受到任何人士偷窺或閉路電視的監視；
- 強烈建議使用者擁有僅用於存取恒生HSBCnet 的專屬終端機，以降低惡意程式碼被加載到裝置的可能性。此裝置不應用於一般的網頁瀏覽、電子郵件或社交網絡；
- 切勿向閣下的任何員工或組織內部透露任何安全憑證。 閣下應謹慎留意任何聲稱來自銀行或任何第三方要求披露任何密碼、使用者安全憑證或任何帳戶詳細資料的信件或通訊。 一旦發生此事，閣下必須儘快向銀行在發生任何可疑活動、任何顧慮或可疑信件或通訊時立即向銀行報告；
- 請確保，倘若閣下懷疑憑證以任何方式遭到全部或部分洩漏，請立即採取妥善行動，藉由變更憑證或在採取妥善行動時暫停使用者，以保護其使用者的設定檔。一旦閣下懷疑任何憑證已被洩漏時，也應儘快檢查其銀行帳戶最近的活動以及使用者設定檔，藉此識別任何未經授權的行為；且
- 閣下有責任定期審查其銀行帳戶及使用者設定檔活動，以確保不存在任何違規行為，倘若發現任何違規行為，閣下必須立即通知銀行。

系統相容性

閣下必須確保擁有兼容的硬體及軟體以便存取相關的恒生HSBCnet。恒生HSBCnet客戶指南中詳列了最低系統需求。
閣下同意操作資訊技術及系統控制項目時遵守相關法律及規定，例如沙賓法案(Sarbanes–Oxley)。

安全標準

閣下必須定期審查其內部安全措施，藉此確保所有保護措施保持在最新狀態，並符合法規及業界最佳實踐指南。尤其包括但不限於：

- 閣下使用與恒生HSBCnet相關的加密技術必須符合使用者存取恒生HSBCnet所在地的當地法律;
- 閣下應使用並維護垃圾郵件過濾器，桌面防火牆，以及即時防毒軟件。收到更新時，必須在相應的時間間隔內更新這些工具，並用來掃描閣下的電腦;
- 閣下應在操作系統及所有應用程式的安全性更新及應用程式修補程式推出時，立即更新且安裝；
- 切勿使用公共網際網路存取點(例如網吧，公共Wi-Fi熱點) 來存取恒生HSBCnet或閣下的帳戶或個人資訊。若必須使用這些存取點，則請務必採用VPN (虛擬專用網絡)。

恒生HSBCnet 存取

為防止未經授權存取恒生 HSBCnet 及 / 或降低閣下遭受任何潛在安全威脅的風險，閣下必須確保：

a) 使用者在使用後登出恒生HSBCnet，並在登入恒生HSBCnet時不允許存取這些終端機；
b) 使用者要按照指定的登出流程（在恒生HSBCnet內，使用者應選擇螢幕右上角的「登出」按鈕），正確登出恒生HSBCnet，而非僅僅關閉瀏覽器視窗； 以及
c) 尚未確認來電者身份前，閣下切勿在電話中提供任何資訊。 閣下有責任透過獨立方式，亦即聯繫公開線路或已知聯繫人，聯絡銀行蒐集資料，並確認來電者的身份。銀行絕不會要求閣下提供任何密碼資訊。

若有任何未經授權，或可疑的存取或使用恒生 HSBCnet（包括憑證），或任何未經授權、未知或可疑的交易、通訊或指令發生，閣下必須立即通知銀行。
若閣下遇到下列情況時必須立即通知銀行：

- 其存取恒生 HSBCnet 的瀏覽器出現異常及 / 或無回應；
- 發現內容顯示方式有變化;
- 收到銀行提供的安全憑證後，又收到訊息表示系統無法使用;
- 在操作時段期間，收到未預期的訊息，要求提供安全憑證或電子簽章；
- 收到不尋常的彈出訊息； 或
- 發現新的或未預期的工具列及 / 或圖示

若閣下發現可疑活動，必須立即停止在恒生 HSBCnet 的所有線上活動，並從網絡中刪除任何可能受到入侵的電腦系統。

當使用具備簽署功能的安全裝置執行電子簽署時，使用者必須核實系統要求其簽名的資料正確無誤（亦即系統要求他們透過恒生 HSBCnet 簽署的受款人帳號，與內部付款系統或文件上的資料一致）。若發現網上提供的資訊與實際活動詳情有出入，閣下必須立即通知銀行。

使用者在使用恒生 HSBCnet 及 / 或任何可以透過恒生 HSBCnet存取的產品或工具時，有任何實際或可疑的不當情況，或使用者已無權使用恒生HSBCnet（由於離職或其他原因）時，閣下必須立即移除其使用者的存取權限，並立即通知銀行。

為了找出實際或潛在安全性違規事件，閣下必須遵守銀行、警方或其他監管機構所提出的合理要求。 閣下必須對透過恒生 HSBCnet，每日執行款項對帳的指示。

暫停使用者

恒生 HSBCnet 允許系統管理員暫停其他使用者的帳戶。 此功能僅限於需要令使用者暫時無法使用恒生 HSBCnet 的情況下使用，例如放假。此功能的目的不是於使用者行為存有重大安全疑慮時使用。 在此情況下，系統管理員應立即從恒生 HSBCnet 刪除該使用者的帳戶，並撤銷該使用者的實體保安編碼器（如持有）或流動保安編碼器。

若暫停是唯一可用的選項（例如：因為必須緊急停用該使用者，且沒有其他系統管理員可以批核刪除指示），則應與其他保護措施一併執行（例如：取回使用者的實體保安編碼器（如持有））。 如有疑問，請致電銀行尋求協助。 使用者需要處於「啟用中」或「已批核」的狀態下才能被暫停。一旦使用者被暫停，於重新啟用或刪除前，切勿對該使用者的帳戶或存取權限進行任何維護。

恒生HSBCnet 流動理財服務

除了遵守一般電子管道安全性措施的義務外，閣下還必須確保遵守與流動裝置上的恒生 HSBCnet 流動理財應用程式相關的附加安全要求**，包括:

- 不要在流動裝置上儲存閣下的恒生HSBCnet登入或個人資料。
- 使用流動裝置連接到無線網絡時，僅使用受信任的網絡或服務供應商，並啟用額外的安全保護，例如Wi-Fi Protected Access (WPA)。
- 旅行時，盡可能使用可靠的電腦或流動裝置。確保閣下的裝置已安裝最新的製造商軟件更新，並避免使用「已越獄」的裝置，或「已取得 root 權限」並未經授權修改的裝置。
- 請勿與他人共用流動裝置。為防止他人盜用裝置，請啟用密碼 / PIN 碼鎖定功能。
- 使用安全性強，且黑客無法輕易猜測或推斷的 PIN 碼，並定期更改 PIN 碼。閣下可以隨時在恒生 HSBCnet流動理財應用程式設置中更新閣下的HSBCnet保安密碼。
- 登入恒生 HSBCnet流動理財應用程式後，請不要離開或閒置閣下的流動裝置。當使用完後，請確保閣下已完全登出恒生 HSBCnet流動理財服務及關閉程式。
- 不要在閣下的流動裝置上安裝來源不明的應用程式。

** 有關閣下使用恒生HSBCnet流動理財應用程式的安全義務的完整詳情， 請參閱**「電子管道安全性措施」**。