保護資料

資料私隱

政策及原則

我們致力根據營運所在市場的相關法律及規例，保護及尊重我們所持有和處理的資料。本行的方針建基於具備適當的人才、技術、系統、監控措施、政策及流程，確保私隱風險得到恰當管理。就管理資料私隱風險而言，集團層面的私隱政策及原則旨在為我們提供全球一致的方針，所有環球業務及環球部門均須遵守該等政策及原則。

我們已制訂多項程序，清晰說明處理資料私隱考慮事項時須採取的行動，當中包括發生須呈報的事件時，按適用私隱法律及規例通知監管機關、客戶或其他資料當事人。

本行政策涵蓋集團私隱政策原則等多項原則，列明我們應如何在高級管理層面處理資料私隱風險。該等原則及風險管理方針的落實程序與本行的監控機制維持一致。

我們定期就資料私隱風險展開風險及監控評估，並將具備詳情記入本行的非財務風險記錄系統。我們已就資料私隱風險及其他資料風險成立正規管治論壇，協助高級管理人員作出積極的風險管理決策。

我們已制訂私隱政策原則，以管理資料私隱風險。私隱政策原則旨在：

- 訂立良好的資料私隱慣例
- 展示我們遵守私隱法律及法規，並對守法負責
- 說明本行處理可識別資料的承諾

我們已實施以下數項控制措施，以管理資料私隱風險。

處理記錄	了解本行處理的可識別資料，詳細記錄本行如何處理可識別資料，並保存有關過程的證據，以確保本行能夠證明其遵守相關資料私隱法例。
私隱影響性評估	確保及時識別由可識別資料的新用途或處理變動所導致的資料私隱風險，並確保所識別的風險在可識別資料應用作任何新用途或出現處理變動前得到妥善管理。
內部及外部資料轉移	確保任何可識別資料的轉移均獲得批准，並符合資料私隱相關法例及本行有關資料私隱的政策，當中涵蓋內部轉移（任何司法管轄區的集團實體之間的資料轉移）及外部轉移。
資料披露	確保可識別數據的外部披露（通常應外部要求作出）得到及時、一致、合規和準確的處理，並遵守相關資料私隱法例。
個人私隱權利	當個人或其代表就本行持有的資料行使權利時，確保本行能夠及時、合規地作出回應，並遵守相關資料私隱法例。
私隱通知	確保我們根據相關資料私隱法例，清晰及透明地向個人提供有關公平及合法處理可識別資料的聲明。
同意及選擇	確保我們根據相關資料私隱法例，獲取處理可識別資料所需之同意，並持續予以更新和管理。

客戶私隱

我們通知客戶有關我們收集和使用個人資料的目的、資料轉移對象類別、市場推廣對象類別、以及其存取和更正資料的權利。他們可隨時瀏覽本行網站，查閱我們的私隱政策、《致各客戶及其他個別人士關於個人資料（私隱）條例的通知》及《Cookies政策》。

我們明白，員工在保障本行持份者免受數據安全及資料私隱風險影響方面扮演重要的角色。我們以裝備每位員工為己任，致力為所有同事提供所需的合適工具和指引，讓組織及客戶的安全得到保障。我們為本行上下所有員工提供網絡安全及資料私隱培訓，對象涵蓋高級管理層乃至前線客戶經理，務求提升員工的數據安全及資料私隱意識。

我們亦每年為員工舉辦培訓課程，課程涵蓋數據安全、資料私隱風險及相關監控措施方面的特定議題。

本行網站設有專門介紹數據安全監控措施的頁面，提醒客戶騙徒可能使用詐騙伎倆盜取其個人資料，因此他們務必時刻警覺，慎防欺詐活動。該頁面亦提供提防偽冒來電和手機短訊的貼士，以協助客戶避免成為受害者。

所有員工在得知重大事故後都必須根據重大事故上報手冊，立即向業務風險及控制管理部門或控制總監辦公室團隊報告事故詳情。相關專責人員獲悉後會展開調查，並在適當的情況下將問題上報至核心小組。為持續改善本行的業務表現，專責人員亦會就如何控制及回應事件提供建議，並制訂補救措施和總結事件中汲取的經驗。

*獲確證實的客戶私隱投訴**

接獲渠道	
外部人士	0
本行	8
監管機構	0
總計	**8**

類型	
私隱洩漏	6
失竊	0
遺失客戶資料	2
其他	0
總計	**8**

* 獲確證實的客戶私隱投訴個案即已經過內部調查並確定的個案。

網絡安全

科技的廣泛應用以及我們對其的依賴，令網絡威脅快速進化，本來有效降低網絡安全風險的控制措施隨時間推移變得過時。我們的監管機構、顧客及客戶期望我們採取必要措施，以業內最佳標準保護市場、他們的數據及業務利益。我們於過去數年不斷在網絡安全上投放資源，以達致良好實踐標準，未來將致力維持此標準。

我們需要不斷檢討本行的網絡風險偏好，並維持監控措施在減輕相關風險方面的長期成效，方可在時下網絡威脅不斷升級的環境下維持一貫的良好標準。儘管在大多數情況下，降低網絡攻擊的潛在影響極為困難，但透過在持續監控上投放資源，減低整體網絡風險並非不可能的事。本行持續重新評估監控措施的成效，並透過投資於維持和加強此等監控措施，從而將剩餘風險維持在可接受的水平。

我們繼續投放資源於防禦日益複雜的網絡攻擊，重點加強異常事件偵測、事故應對流程、安全開發和網絡系統漏洞修復，並提升針對惡意軟件、應用程式層攻擊及數據洩漏的防護。此外，我們已透過進行網絡安全盡職審查加強我們的第三方管理，以實現更嚴格的管治系統和措施，例如在批准合約前執行第三方安全測試。

我們日常營運的資訊科技基建全面採用美國國家標準暨技術研究院（「NIST」）網絡安全框架的業界標準。銀行是網絡罪犯的主要目標，這些罪犯可能會嘗試竊取經濟利益和個人資料，從而導致營運中斷、財務損失、聲譽受損和客戶流失。因此，我們以保護本行及客戶免受該等網絡犯罪威脅為首任。

我們的風險管治論壇定期舉行會議，如董事會授權的風險委員會及風險管理會議，確保我們的管治及監控架構得到妥善執行、管理、維持和傳達。為保障我們的營運免受合規風險影響，我們亦制訂了穩健透明的企業管治措施。

我們定期向董事會及高級管理層匯報網絡安全相關的策略計劃及關鍵指標，以協助他們監督本行的網絡安全表現。本行會檢討其網絡安全策略，並討論業務的網絡安全風險狀況、風險緩解意識、內部及外部網絡安全事件及監管要求等事宜。

保護資料

我們亦會為董事會及高級管理層安排網絡安全演習，排演發生重大網絡安全事故時可能需要採取的決策形式，並再三確認所有人員的個別職務及職責。我們定期展開網絡安全演習，以協助本行上下人員進一步了解各自在發生網絡攻擊時應扮演的角色，以及應採取的協議流程、內部溝通途徑及上報程序。我們亦定期展開網絡釣魚測試，以提高組織各部門的整體安全意識。

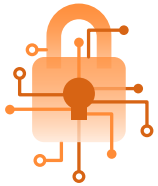
本行設有24小時熱線服務，供員工即時報告網絡安全事故。本行的網絡安全分析員及保安營運中心會調查相關事件，並向管理人員報告，以就補救措施尋求指引。此外，我們亦制訂了網絡安全事故應對程序，並定期加以測試。

網絡安全培訓方面，我們為所有用戶（包括行政人員及其助理、資訊科技系統終端使用者、軟件開發人員及第三方服務供應商等）提供自動化網絡安全評估工具。我們亦透過中央平台管理網絡系統、操作系統、應用程式層和內部自定義軟件的安全漏洞，並根據輕重緩急次序加以修復。

我們於2023年定期或按需要向所有員工提供有關數據安全的網絡安全意識培訓。培訓主題涵蓋數據安全、電子郵件保安及網絡釣魚攻擊、訪問權限控制、事故匯報及上報、安全使用通訊裝置及社交媒體、資訊分類及標籤等。

本行於2023年提供的網絡安全培訓及資訊包括：

- 向全體員工提供的強制性網上培訓
- 向董事會及執行委員會成員提供網絡安全簡介
- 向在環球業務部門及環球職能部門中負責有效管理資訊安全風險的要員提供特定職位培訓
- 向行政助理及資訊科技人員提供培訓
- 由資深管理層及專家講者主持的網絡安全研討會



>99%

員工已按時完成強制性網絡安全培訓

>90%

資訊科技開發人員持有本行至少一項內部安全開發人員認證