BẢNG TÓM TẮT CÁC NỘI DUNG ĐIỀU CHỈNH

ĐIỀU KHOẢN VÀ ĐIỀU KIỆN

(Sự thay đổi này có hiệu lực từ 24/02/2021)

A. Khách Hàng Cá Nhân

Các Điều Khoản và Điều Kiện hiện tại	Các Điều Khoản và Điều Kiện có hiệu lực từ 24/02/2021
***Lưu ý:** Nội dung không có trong bản Điều Khoản và Điều Kiện hiện tại*	***Lưu ý:** Nội dung màu đỏ là phần cập nhật được bổ sung*
CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN CHUNG	**CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN CHUNG**
5. DỮ LIỆU GIAO DỊCH VÀ THÔNG BÁO 5.8. Khách Khách Hàng đảm bảo rằng tất cả các thông tin cung cấp cho Ngân Hàng (bất kể trong Đơn Mở Tài Khoản hay theo cách khác), theo sự hiểu biết cao nhất của Khách Hàng, là chính xác và cập nhật. Khách Hàng cam kết sẽ thông báo cho Ngân Hàng về bất kỳ thay đổi nào đối với các thông tin này, bao gồm nhưng không giới hạn việc Khách Hàng phải thông báo cho Ngân Hàng không chậm trễ bất kỳ thay đổi nào về tên và địa chỉ của Khách Hàng, Chủ Tài Khoản, cũng như việc chấm dứt, hoặc sửa đổi, bất kỳ thẩm quyền đại diện nào trước Ngân Hàng đã được giao cho bất kỳ người nào. Khách hàng theo đây ủy quyền và đồng ý cho Ngân hàng được quyền cập nhật tình trạng cư trú của Khách Hàng căn cứ theo thông tin/ hồ sơ cung cấp từ phía Khách hàng theo phương thức mà Ngân hàng cho là phù hợp.	**5. DỮ LIỆU GIAO DỊCH VÀ THÔNG BÁO** 5.8 Khách Hàng đảm bảo rằng tất cả các thông tin cung cấp cho Ngân Hàng (bất kể trong Đơn Mở Tài Khoản hay theo cách khác), theo sự hiểu biết cao nhất của Khách Hàng, là chính xác và cập nhật. Khách Hàng cam kết sẽ thông báo cho Ngân Hàng về bất kỳ thay đổi nào đối với các thông tin này, bao gồm nhưng không giới hạn việc Khách Hàng phải thông báo cho Ngân Hàng không chậm trễ bất kỳ thay đổi nào về tên và địa chỉ của Khách Hàng, Chủ Tài Khoản, cũng như việc chấm dứt, hoặc sửa đổi, bất kỳ thẩm quyền đại diện nào trước Ngân Hàng đã được giao cho bất kỳ người nào. Khách hàng theo đây ủy quyền và đồng ý cho Ngân hàng được quyền cập nhật tình trạng cư trú và những thông tin khác (họ tên, ngày sinh, số chứng minh nhân dân/ căn cước công dân/ hộ chiếu cùng ngày/ tháng/ năm/ nơi phát hành, địa chỉ) của Khách Hàng căn cứ theo thông tin/ hồ sơ cung cấp từ phía Khách hàng theo

	phương thức mà Ngân hàng cho là phù hợp và không cần thêm bất kỳ sự đồng ý bằng văn bản nào từ Khách hàng. Việc cập nhật này bao gồm cả trường hợp viết tắt hoặc sai khác giữa thông tin trên Chỉ Thị của Khách hàng so với hồ sơ cung cấp từ phía Khách hàng, mà trong đó thông tin trên hồ sơ được cung cấp từ phía Khách hàng là cơ sở đối chiếu theo quy định của Ngân hàng.
CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN DÀNH CHO NGÂN HÀNG TRỰC TUYẾN	**CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN DÀNH CHO NGÂN HÀNG TRỰC TUYẾN**
CHÚ Ý! Xin vui lòng đọc kỹ các nghĩa vụ bảo mật quy định tại các Khoản 3 và 10 dưới đây. Nếu Khách hàng vi phạm bất cứ nghĩa vụ bảo mật nào thì Khách hàng sẽ phải chịu trách nhiệm về các giao dịch kể cả khi Khách hàng không giao kết các giao dịch đó. Các Điều khoản và Điều kiện này ("Điều khoản") giải thích các trách nhiệm và nghĩa vụ của Khách hàng liên quan tới các dịch vụ và thông tin mà Khách hàng sử dụng hoặc được Ngân Hàng yêu cầu hoặc dịch vụ và thông tin mà Ngân Hàng cung cấp cho Khách hàng thông qua Ngân hàng Trực tuyến Cá nhân thuộc dịch vụ Ngân hàng Trực tuyến của HSBC.	**CHÚ Ý!** Xin vui lòng đọc kỹ các Điều khoản và điều kiện này, đặc biệt là các quy định về nghĩa vụ bảo mật quy định tại các Khoản 3 và 10 dưới đây. Nếu Khách Hàng vi phạm bất cứ nghĩa vụ bảo mật nào thì Khách Hàng sẽ phải chịu trách nhiệm về các giao dịch kể cả khi Khách Hàng không giao kết các giao dịch đó. Các Điều khoản và Điều kiện này quy định và giải thích các trách nhiệm và nghĩa vụ của Khách Hàng liên quan tới các dịch vụ và thông tin mà Khách Hàng sử dụng hoặc được Ngân Hàng yêu cầu hoặc dịch vụ và thông tin mà Ngân Hàng cung cấp cho Khách Hàng thông qua Ngân hàng Trực tuyến Cá nhân thuộc dịch vụ Ngân hàng Trực tuyến của HSBC.
1. VỀ BẢN CHẤP THUẬN NÀY	**1. VỀ BẢN CHẤP THUẬN NÀY**
N/A	"**Digital Secure Key**" hoặc "**Tính năng Digital Secure Key**" có nghĩa là một tính năng bảo mật hoạt động trên Ứng dụng HSBC Việt Nam, tính năng này được thiết kế để sử dụng cho việc khởi tạo Mã Bảo mật (các Mật khẩu sử dụng một lần) để truy cập và giao dịch qua các dịch vụ Ngân hàng Trực tuyến Cá nhân.

N/A	"**Ứng dụng HSBC Việt Nam**" hoặc "**Ứng dụng ngân hàng di động HSBC Việt Nam**" có nghĩa là ứng dụng di động được cung cấp và cập nhật liên tục bởi Ngân hàng, có thể được tải về trên bất kỳ thiết bị di động nào chạy những hệ điều hành được Ngân Hàng hỗ trợ theo từng thời điểm, mà thông qua ứng dụng đó Khách hàng có thể truy cập các dịch vụ ngân hàng khả dụng trên ứng dụng của Ngân Hàng. Việc sử dụng ứng dụng HSBC Việt Nam tuân thủ theo Điều khoản và Điều kiện sử dụng ứng dụng HSBC Mobile Banking.
N/A	"**Thiết bị di động**" có nghĩa là một thiết bị di động thông minh, bao gồm điện thoại thông minh (Smartphone), máy tính bảng (Tablet), …)
N/A	"**Thiết bị di động được hỗ trợ**" hoặc "**Thiết bị di động tương thích**" có nghĩa là một thiết bị di động thông minh sử dụng những hệ điều hành được Ngân hàng hỗ trợ để có thể cài đặt ứng dụng HSBC Việt Nam.
"**Mã Bảo mật**" có nghĩa là mật khẩu sử dụng một lần được khởi tạo bởi Thiết bị Bảo mật	**"Mã Bảo mật"** có nghĩa là mật khẩu sử dụng một lần được khởi tạo bởi Thiết Bị Bảo Mật hoặc Digital Secure Key.
N/A	"**Phương thức khởi tạo mã bảo mật**" có nghĩa là cách thức và phương pháp tiến hành khởi tạo Mã Bảo mật bằng cách sử dụng Thiết Bị Bảo Mật hoặc Digital Secure Key.
"Tài khoản" có nghĩa là các tài khoản Ngân Hàng gắn liền với Tên đăng nhập, Mật khẩu (nếu áp dụng), và Thiết bị Bảo mật đã được cung cấp cho Khách hàng để sử dụng dịch vụ.	**"Tài khoản"** có nghĩa là các tài khoản Ngân Hàng gắn liền với Tên đăng nhập, Mật khẩu (nếu áp dụng), và Thiết Bị Bảo Mật đã được cung cấp cho Khách Hàng để sử dụng dịch vụ hoặc Digital Secure Key mà Khách Hàng đã kích hoạt thành công để thay thế Thiết Bị Bảo Mật.
3. NGHĨA VỤ BẢO MẬT CỦA KHÁCH HÀNG	**3. NGHĨA VỤ BẢO MẬT CỦA KHÁCH HÀNG**

b. Để sử dụng các dịch vụ, Khách Hàng sẽ cần một nhận dạng riêng (Tên đăng nhập), một thiết bị bảo mật (Thiết Bị Bảo Mật) và, nếu được yêu cầu, một Mật khẩu.	b. Để sử dụng các dịch vụ, Khách Hàng sẽ cần một nhận dạng riêng (Tên đăng nhập), một Thiết Bị Bảo Mật hoặc Thiết bị di động đã cài Ứng dụng HSBC Việt Nam với tính năng Digital Secure Key đang hoạt động và, nếu được yêu cầu, một Mật khẩu.
N/A	c. Khách hàng là người duy nhất có trách nhiệm cân nhắc kỹ lưỡng và lựa chọn Thiết Bị Bảo Mật/ Digital Secure Key sao cho phù hợp với nhu cầu sử dụng của mình. Mỗi tài khoản Ngân hàng Trực tuyến Cá nhân gắn liền với một Tên tài khoản chỉ được quyền sử dụng duy nhất một phương thức khởi tạo mã bảo mật tại một thời điểm.
N/A	e. Khách hàng là người duy nhất có trách nhiệm kích hoạt tính năng Digital Secure Key để thay thế Thiết Bị Bảo Mật trong việc khởi tạo mã bảo mật
f. Để Thiết lập lại Mật khẩu Trực tuyến, Khách hàng cần cung cấp cho Ngân Hàng Tên đăng nhập, hoàn thành các Câu hỏi để Thiết lập lại Mật khẩu và cung cấp xác nhận sử dụng Thiết bị Bảo mật.	h. Để Thiết lập lại Mật khẩu Trực tuyến, Khách Hàng cần cung cấp cho Ngân Hàng Tên đăng nhập, hoàn thành các Câu hỏi để Thiết lập lại Mật khẩu và cung cấp xác nhận sử dụng Thiết Bị Bảo Mật/ Digital Secure Key.
h. Khách hàng phải giữ bí mật Mật khẩu của mình và bảo mật cho Mật khẩu đó và thực hiện các biện pháp hợp lý để ngăn chặn việc sử dụng trái phép Tên đăng nhập, Mật khẩu, Câu hỏi để Thiết lập lại Mật khẩu và Mã Bảo mật của Khách hàng. Khách hàng không được để người khác chiếm hữu hoặc điều khiển Thiết bị Bảo mật trong bất kì tình huống nào và vào bất kì thời điểm nào.	j. Khách Hàng phải giữ bí mật Mật khẩu của mình và bảo mật cho Mật khẩu đó và thực hiện các biện pháp hợp lý để ngăn chặn việc sử dụng trái phép Tên đăng nhập, Mật khẩu, Câu hỏi để Thiết lập lại Mật khẩu và Mã Bảo mật của Khách Hàng. Khách Hàng không được để người khác chiếm hữu hoặc điều khiển Thiết Bị Bảo Mật hoặc Thiết bị di động được dùng để sử dụng tính năng Digital Secure Key trong bất kì tình huống nào và vào bất kì thời điểm nào.

j. Khách hàng phải thông báo cho Ngân Hàng ngay lập tức về bất kì việc kết nối trái phép nào vào các dịch vụ hoặc về bất kì giao dịch hoặc yêu cầu trái phép nào mà Khách hàng biết hoặc nghi ngờ hoặc nếu Khách hàng nghi ngờ ai đó biết Tên đăng nhập, Mật khẩu, Câu hỏi để Thiết lập lại Mật khẩu và Mã Bảo mật hoặc chiếm hữu, điều khiển hoặc sử dụng Thiết bị Bảo mật.	l. Khách Hàng phải thông báo cho Ngân Hàng ngay lập tức về bất kì việc kết nối trái phép nào vào các dịch vụ hoặc về bất kì giao dịch hoặc yêu cầu trái phép nào mà Khách Hàng biết hoặc nghi ngờ hoặc nếu Khách Hàng nghi ngờ ai đó biết Tên đăng nhập, Mật khẩu, Câu hỏi để Thiết lập lại Mật khẩu và Mã Bảo mật hoặc chiếm hữu, điều khiển hoặc sử dụng Thiết Bị Bảo Mật hoặc Thiết bị di động được dùng để sử dụng tính năng Digital Secure Key.
6. CẤM SỬ DỤNG DỊCH VỤ	**6. CẤM SỬ DỤNG DỊCH VỤ**
b. Khách hàng không được (và không được cố gắng) phá rối hoặc quấy nhiễu dưới bất kì hình thức nào bất kì một phần nào của các dịch vụ (bao gồm trang mạng trực tuyến, Thiết bị Bảo mật hay phần mềm liên quan tới Ngân Hàng hoặc các dịch vụ). Khách hàng không được (và không được cố gắng) kết nối vào bất kì thứ gì liên quan tới các dịch vụ (bao gồm trang mạng trực tuyến hay phần mềm liên quan tới Ngân Hàng hoặc các dịch vụ mà Ngân Hàng không định để Khách hàng kết nối) bao gồm bất kì thứ gì được bảo vệ, trừ khi sử dụng Tên đăng nhập, Mã Bảo mật, Mật Khẩu (nếu áp dụng) và Câu hỏi để Thiết lập lại Mật khẩu.	b. Khách Hàng không được (và không được cố gắng) phá rối hoặc quấy nhiễu dưới bất kì hình thức nào bất kì một phần nào của các dịch vụ (bao gồm trang mạng trực tuyến, Thiết Bị Bảo Mật, Ứng dụng HSBC Việt Nam, tính năng Digital Secure Key hay phần mềm liên quan tới Ngân Hàng hoặc các dịch vụ). Khách Hàng không được (và không được cố gắng) kết nối vào bất kì thứ gì liên quan tới các dịch vụ (bao gồm trang mạng trực tuyến hay phần mềm liên quan tới Ngân Hàng hoặc các dịch vụ mà Ngân Hàng không định để Khách Hàng kết nối) bao gồm bất kì thứ gì được bảo vệ, trừ khi sử dụng Tên đăng nhập, Mã Bảo mật, Mật Khẩu (nếu áp dụng) và Câu hỏi để Thiết lập lại Mật khẩu.
10. TRÁCH NHIỆM CỦA KHÁCH HÀNG ĐỐI VỚI CÁC GIAO DỊCH KHÔNG ĐÚNG THẨM QUYỀN	**10. TRÁCH NHIỆM CỦA KHÁCH HÀNG ĐỐI VỚI CÁC GIAO DỊCH KHÔNG ĐÚNG THẨM QUYỀN**
b. Nếu Khách hàng để bất kì người nào sử dụng một hay nhiều những mục sau: i) Tên đăng nhập, ii) Mật khẩu, iii) Các Câu hỏi để Thiết lập lại Mật khẩu, iv) Thiết bị Bảo mật và/hoặc v) Mã Bảo mật của	b. Nếu Khách Hàng để bất kì người nào sử dụng một hay nhiều những mục sau: i) Tên đăng nhập, ii) Mật khẩu, iii) Các Câu hỏi để Thiết lập lại Mật khẩu, iv) Thiết Bị Bảo Mật/ Digital Secure Key và/hoặc

Khách hàng thì Khách hàng sẽ phải chịu trách nhiệm đối với tất cả các khiếu nại, tổn thất và hậu quả phát sinh từ hoặc liên quan tới tất cả các giao dịch được tiến hành thông qua việc sử dụng các dịch vụ bởi hoặc với sự đồng ý của người đó.	v) Mã Bảo mật của Khách Hàng thì Khách Hàng sẽ phải chịu trách nhiệm đối với tất cả các khiếu nại, tổn thất và hậu quả phát sinh từ hoặc liên quan tới tất cả các giao dịch được tiến hành thông qua việc sử dụng các dịch vụ bởi hoặc với sự đồng ý của người đó.
c. Nếu Khách hàng có tham gia vào một giao dịch không đúng thẩm quyền, Khách hàng sẽ phải chịu trách nhiệm về một số hoặc tất cả các tổn thất phát sinh từ giao dịch không đúng thẩm quyền đó. Các cách mà Khách hàng tham gia vào một giao dịch không đúng thẩm quyền bao gồm cả việc không thực hiện các bước hợp lý để theo dõi bất kì nghĩa vụ bảo mật nào được đề cập đến trong các Điều khoản này và/hoặc bất kì một sự chậm trễ không chính đáng nào trong việc thông báo cho Ngân Hàng về việc tiết lộ hoặc khả năng tiết lộ cho người khác Tên đăng nhập hoặc Mật khẩu hoặc các Câu hỏi để Thiết lập lại Mật khẩu hoặc Mã Bảo mật và/hoặc việc sử dụng, điều khiển không đúng thẩm quyền hoặc mất Thiết bị Bảo mật của Khách hàng.	c. Nếu Khách Hàng có tham gia vào một giao dịch không đúng thẩm quyền, Khách Hàng sẽ phải chịu trách nhiệm về một số hoặc tất cả các tổn thất phát sinh từ giao dịch không đúng thẩm quyền đó. Các cách mà Khách Hàng tham gia vào một giao dịch không đúng thẩm quyền bao gồm cả việc không thực hiện các bước hợp lý để theo dõi bất kì nghĩa vụ bảo mật nào được đề cập đến trong các Điều khoản này và/hoặc bất kì một sự chậm trễ không chính đáng nào trong việc thông báo cho Ngân Hàng về việc tiết lộ hoặc khả năng tiết lộ cho người khác Tên đăng nhập hoặc Mật khẩu hoặc các Câu hỏi để Thiết lập lại Mật khẩu hoặc Mã Bảo mật và/hoặc việc sử dụng, điều khiển không đúng thẩm quyền hoặc mất Thiết Bị Bảo Mật/ Thiết bị di động được dùng để sử dụng Tính năng Digital Secure Key của Khách Hàng.
d. Nếu Khách hàng đã thông báo sớm trong khả năng có thể cho Ngân Hàng về việc tiết lộ hoặc khả năng tiết lộ cho người khác Tên đăng nhập hoặc Mật khẩu hoặc các Câu hỏi để Thiết lập lại Mật khẩu hoặc Mã Bảo mật và/hoặc việc sử dụng, điều khiển không đúng thẩm quyền hoặc mất Thiết bị Bảo mật của Khách hàng thì Khách hàng sẽ không phải chịu trách nhiệm đối với các tổn thất phát sinh sau khi Ngân Hàng đã nhận được thông báo đó trừ khi Khách Hàng hành động một cách cố ý hoặc bất cẩn.	d. Nếu Khách Hàng đã thông báo sớm trong khả năng có thể cho Ngân Hàng về việc tiết lộ hoặc khả năng tiết lộ cho người khác Tên đăng nhập hoặc Mật khẩu hoặc các Câu hỏi để Thiết lập lại Mật khẩu hoặc Mã Bảo mật và/hoặc việc sử dụng, điều khiển không đúng thẩm quyền hoặc mất Thiết Bị Bảo Mật/ Thiết bị di động được dùng để sử dụng Tính năng Digital Secure Key của Khách Hàng thì Khách Hàng sẽ không phải chịu trách nhiệm đối với các tổn thất

	phát sinh sau khi Ngân Hàng đã nhận được thông báo đó trừ khi Khách Hàng hành động một cách cố ý hoặc bất cẩn.
11. THIẾT BỊ BẢO MẬT	**11. THIẾT BỊ BẢO MẬT/ DIGITAL SECURE KEY**
Ngân Hàng sẽ nỗ lực hợp lí để bảo đảm rằng Thiết bị Bảo mật đã cung cấp cho Khách hàng sẽ hoạt động ở mức cần thiết để cho phép kết nối với các dịch vụ khi được yêu cầu. Khách hàng phải thông báo cho Ngân Hàng ngay lập tức nếu bất kì Thiết bị Bảo mật nào không hoạt động đúng chức năng và nghĩa vụ duy nhất của Ngân Hàng đối với Thiết bị Bảo mật đó là thay thế nó bởi một Thiết bị Bảo mật mới với mức phí mà Ngân Hàng sẽ quy định tùy từng thời điểm, ngoại trừ trong các trường hợp dưới đây: a. Thiết bị Bảo mật có lỗi được chuyển trả cho Ngân Hàng trong vòng 90 ngày kể từ ngày được cấp; và b. Ngân Hàng có bằng chứng là Khách hàng không có lỗi hoặc bất cẩn dẫn đến hoặc góp phần làm cho Thiết bị Bảo mật không hoạt động đúng chức năng. Trừ những điều quy định trong Khoản 11(a) này, Ngân Hàng sẽ không chịu trách nhiệm liên quan tới Thiết bị Bảo mật, bao gồm cả trách nhiệm đối với việc vi phạm bất kì điều khoản ngụ ý nào về chất lượng phù hợp, sự vận hành hay sự thích hợp cho một mục đích nào đó của bất kì Thiết bị Bảo mật nào. Ngoài ra, Ngân hàng không thể chịu trách nhiệm về bất kì mất mát hay tổn thất nào mà Khách hàng gặp phải hay phải gánh chịu do việc Khách hàng không giữ bảo mật và/hoặc không sử dụng Thiết bị Bảo mật đúng theo Yêu cầu và khuyến cáo của Ngân Hàng.	a. Ngân Hàng sẽ nỗ lực hợp lí để bảo đảm rằng Thiết bị Bảo mật đã cung cấp cho Khách hàng sẽ hoạt động ở mức cần thiết để cho phép kết nối với các dịch vụ khi được yêu cầu. b. Khách hàng phải thông báo cho Ngân Hàng ngay lập tức nếu bất kì Thiết bị Bảo mật nào không hoạt động đúng chức năng và nghĩa vụ duy nhất của Ngân Hàng đối với Thiết bị Bảo mật đó là thay thế nó bởi một Thiết bị Bảo mật mới với mức phí mà Ngân Hàng sẽ quy định tùy từng thời điểm, ngoại trừ trong các trường hợp dưới đây: i) Thiết bị Bảo mật có lỗi được chuyển trả cho Ngân Hàng trong vòng 90 ngày kể từ ngày được cấp; và ii) Ngân Hàng có bằng chứng là Khách hàng không có lỗi hoặc bất cẩn dẫn đến hoặc góp phần làm cho Thiết bị Bảo mật không hoạt động đúng chức năng. Trừ những điều quy định trong Khoản 11(a) này, Ngân Hàng sẽ không chịu trách nhiệm liên quan tới Thiết bị Bảo mật, bao gồm cả trách nhiệm đối với việc vi phạm bất kì điều khoản ngụ ý nào về chất lượng phù hợp, sự vận hành hay sự thích hợp cho một mục đích nào đó của bất kì Thiết bị Bảo mật nào. Ngoài ra, Ngân hàng không thể chịu trách nhiệm về bất kì mất mát hay tổn thất nào mà Khách hàng gặp phải hay phải gánh chịu do

	việc Khách hàng không giữ bảo mật và/hoặc không sử dụng Thiết bị Bảo mật đúng theo Yêu cầu và khuyến cáo của Ngân Hàng.
N/A	c. Từ tháng 02 năm 2021, trừ trường hợp Ngân hàng có quyết định khác, tính năng Digital Secure Key là công cụ mặc định (thay thế Thiết Bị Bảo Mật) để tạo Mã bảo mật cho Ngân hàng Trực tuyến Cá nhân. i) Đối với Khách hàng hiện đang sử dụng Thiết Bị Bảo Mật, khi Khách hàng kích hoạt thành công tính năng Digital Secure Key, Thiết Bị Bảo Mật của Khách hàng sẽ lập tức bị mất hiệu lực sử dụng. ii) Khách hàng có thể trì hoãn việc kích hoạt Digital Secure Key trong một khoảng thời gian nhất định ("Thời gian chờ") được quy định cụ thể bởi Ngân hàng tại từng thời điểm. Trong khoảng Thời gian chờ, Khách hàng vẫn có thể sử dụng Thiết Bị Bảo Mật và Ứng dụng HSBC Việt Nam bình thường. iii) Sau Thời gian chờ, nếu Khách hàng vẫn chưa kích hoạt thành công tính năng Digital Secure Key, Khách hàng vẫn có thể tiếp tục sử dụng Thiết Bị Bảo Mật để đăng nhập và sử dụng các dịch vụ khả dụng trên Ngân hàng Trực tuyến Cá nhân, tuy nhiên Khách hàng sẽ không thể truy cập và sử dụng Ứng dụng HSBC Việt Nam cho đến khi Khách hàng kích hoạt thành công tính năng Digital Secure Key.

	iv) Trong trường hợp khách hàng đã kích hoạt Digital Secure Key để sử dụng nhưng sau đó muốn quay về sử dụng Thiết Bị Bảo Mật, với điều kiện Thiết Bị Bảo Mật vẫn tiếp tục được cung cấp/chấp nhận bởi Ngân hàng, Khách hàng sẽ phải tuân theo quy trình của Ngân hàng tại thời điểm đó cho việc thay đổi phương thức tạo mã bảo mật, và chịu mọi khoản phí có thể được áp dụng. v) Khi có bất kỳ thiết bị di động nào của Khách hàng dùng để sử dụng tính năng Digital Secure Key trở nên không thể vận hành bình thường các tính năng cần thiết, bị suy giảm mức độ bảo mật hoặc không thể duy trì việc tuân thủ yêu cầu bảo mật theo hướng dẫn/khuyến nghị của Ngân hàng, hoặc không còn nằm trong quyền kiểm soát của Khách hàng (dù là vô tính hay cố ý) bao gồm (nhưng không giới hạn) các trường hợp như: hư hại, bị thất lạc, mất cắp, thay đổi, bị tấn công can thiệp quyền kiểm soát hoặc đánh cắp dữ liệu, … Khách hàng có trách nhiệm ngay lập tức tự gỡ thiết bị đó khỏi danh sách thiết bị được đăng ký sử dụng Ứng dụng HSBC Việt Nam thông qua: (i) Ứng dụng HSBC Việt nam được cài đặt trên một thiết bị di động tương thích khác (tuỳ vào tình trạng khả dụng của tính năng liên quan trên Ứng dụng HSBC Việt Nam tại từng thời điểm); (ii) liên hệ Trung tâm Dịch vụ Khách hàng của Ngân hàng; hoặc (iii) bất kỳ phương thức nào khác được Ngân hàng áp dụng tại từng thời điểm.
16. CÁC VẤN ĐỀ CHUNG	**16. CÁC VẤN ĐỀ CHUNG**

c. Bồi hoàn: Bằng việc kết nối, sử dụng và/hoặc tiếp tục sử dụng Trang mạng của các dịch vụ này, Khách Hàng thể hiện sự đồng ý sẽ bồi hoàn và bảo đảm cho HSBC, giám đốc, nhân viên, người được chỉ định và đại diện của HSBC được bồi hoàn đối với tất cả các hành động, trách nhiệm, chi phí, khiếu nại, mất mát, tổn thất, kiện cáo và/hoặc các khoản phí (bao gồm tất cả các chi phí luật sư trên cơ sở khoản bồi hoàn) mà Ngân Hàng phải gánh chịu hoặc gặp phải bao gồm nhưng không giới hạn, liên quan tới hoặc phát sinh từ: ii) Bất kì yêu cầu không đúng thẩm quyền nào (bao gồm Yêu cầu từ người không có quyền và/hoặc yêu cầu được đưa ra từ việc sử dụng không đúng thẩm quyền Tên đăng nhập Mật khẩu (nếu áp dụng), các Câu hỏi để Thiết lập lại Mật khẩu và/hoặc Mã Bảo mật và/hoặc Thiết Bị Bảo Mật) có thể được truyền qua Ngân hàng Trực tuyến Cá nhân hoặc bất kì yêu cầu không đầy đủ, không chính xác hoặc sai lạc nào; iv) Bất kì vi phạm hoặc việc không tuân thủ bất kì Điều khoản nào của Khách Hàng hoặc của bất kì người không có thẩm quyền nào sử dụng Tên đăng nhập/Mã cá nhân Ngân Hàng Trực tuyến, Mật khẩu, các Câu hỏi để Thiết lập lại Mật khẩu và Thiết Bị Bảo Mật của Khách Hàng;	c. Bồi hoàn: Bằng việc kết nối, sử dụng và/hoặc tiếp tục sử dụng Trang mạng của các dịch vụ này, Khách Hàng thể hiện sự đồng ý sẽ bồi hoàn và bảo đảm cho HSBC, giám đốc, nhân viên, người được chỉ định và đại diện của HSBC được bồi hoàn đối với tất cả các hành động, trách nhiệm, chi phí, khiếu nại, mất mát, tổn thất, kiện cáo và/hoặc các khoản phí (bao gồm tất cả các chi phí luật sư trên cơ sở khoản bồi hoàn) mà Ngân Hàng phải gánh chịu hoặc gặp phải bao gồm nhưng không giới hạn, liên quan tới hoặc phát sinh từ: ii) Bất kì yêu cầu không đúng thẩm quyền nào (bao gồm Yêu cầu từ người không có quyền và/hoặc yêu cầu được đưa ra từ việc sử dụng không đúng thẩm quyền Tên đăng nhập Mật khẩu (nếu áp dụng), các Câu hỏi để Thiết lập lại Mật khẩu và/hoặc Mã Bảo mật và/hoặc Thiết Bị Bảo Mật/ Digital Secure Key) có thể được truyền qua Ngân hàng Trực tuyến Cá nhân hoặc bất kì yêu cầu không đầy đủ, không chính xác hoặc sai lạc nào; iv) Bất kì vi phạm hoặc việc không tuân thủ bất kì Điều khoản nào của Khách Hàng hoặc của bất kì người không có thẩm quyền nào sử dụng Tên đăng nhập/Mã cá nhân Ngân Hàng Trực tuyến, Mật khẩu, các Câu hỏi để Thiết lập lại Mật khẩu và Thiết Bị Bảo Mật/ Digital Secure Key của Khách Hàng;
CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN SỬ DỤNG DỊCH VỤ NGÂN HÀNG QUA ĐIỆN THOẠI HIỆN TẠI	**CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN SỬ DỤNG DỊCH VỤ NGÂN HÀNG QUA ĐIỆN THOẠI**

3. HOẠT ĐỘNG CỦA DỊCH VỤ NGÂN HÀNG QUA ĐIỆN THOẠI	3. HOẠT ĐỘNG CỦA DỊCH VỤ NGÂN HÀNG QUA ĐIỆN THOẠI
Khách Hàng có thể sử dụng Dịch Vụ Ngân Hàng Qua Điện Thoại để: (a) kiểm tra số dư của các Tài Khoản; (b) lấy thông tin về những giao dịch vừa được thực hiện trên Tài Khoản; (c) chuyển tiền từ Tài Khoản Chỉ Định qua Tài Khoản Thẻ Tín Dụng của Khách Hàng nêu trong Dịch Vụ Ngân Hàng Qua Điện Thoại đã được xác định trước về giới hạn chỉ định chuyển khoản; (d) lấy thông tin về các tỷ giá ngoại hối và lãi suất tiền gửi; (e) kích hoạt Thẻ Tín Dụng, bao gồm việc kích hoạt thẻ qua Trung Tâm Dịch Vụ Khách Hàng, Dịch Vụ Ngân Hàng tự động Qua Điện Thoại hoặc tin nhắn SMS theo quy định của Ngân Hàng quy định; (f) tiến hành các dịch vụ ngân hàng và dịch vụ thẻ tín dụng khác mà Ngân Hàng sẽ giới thiệu tại từng thời điểm.	Khách Hàng có thể sử dụng Dịch Vụ Ngân Hàng Qua Điện Thoại để: (a) kiểm tra số dư của các Tài Khoản; (b) lấy thông tin về những giao dịch vừa được thực hiện trên Tài Khoản; (c) chuyển tiền từ Tài Khoản Chỉ Định qua Tài Khoản Thẻ Tín Dụng của Khách Hàng nêu trong Dịch Vụ Ngân Hàng Qua Điện Thoại đã được xác định trước về giới hạn chỉ định chuyển khoản; (d) kích hoạt Thẻ Tín Dụng; Hàng tự động Qua Điện Thoại hoặc tin nhắn SMS theo quy định của Ngân Hàng quy định; (e) tiến hành các dịch vụ ngân hàng và dịch vụ thẻ tín dụng khác mà Ngân Hàng sẽ giới thiệu tại từng thời điểm.

B. Khách Hàng Premier

Các Điều Khoản và Điều Kiện hiện tại	Các Điều Khoản và Điều Kiện có hiệu lực từ 24/02/2021
***Lưu ý:** Nội dung không có trong bản Điều Khoản và Điều Kiện hiện tại*	***Lưu ý:** Nội dung màu đỏ là phần cập nhật được bổ sung*
CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN DÀNH CHO NGÂN HÀNG TRỰC TUYẾN	**CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN DÀNH CHO NGÂN HÀNG TRỰC TUYẾN**
CHÚ Ý! Xin vui lòng đọc kỹ các nghĩa vụ bảo mật quy định tại các Khoản 3 và 10 dưới đây. Nếu Khách hàng vi phạm bất cứ nghĩa vụ bảo mật nào thì Khách hàng sẽ phải chịu trách nhiệm về các giao dịch kể cả khi Khách hàng không giao kết các giao dịch đó. Các Điều khoản và Điều kiện này ("Điều khoản") giải thích các trách nhiệm và nghĩa vụ của Khách hàng liên quan tới các dịch vụ và thông tin mà Khách hàng sử dụng hoặc được Ngân Hàng yêu cầu hoặc dịch vụ và thông tin mà Ngân Hàng cung cấp cho Khách hàng thông qua Ngân hàng Trực tuyến Cá nhân thuộc dịch vụ Ngân hàng Trực tuyến của HSBC.	**CHÚ Ý!** Xin vui lòng đọc kỹ các Điều khoản và điều kiện này, đặc biệt là các quy định về nghĩa vụ bảo mật quy định tại các Khoản 3 và 10 dưới đây. Nếu Khách Hàng vi phạm bất cứ nghĩa vụ bảo mật nào thì Khách Hàng sẽ phải chịu trách nhiệm về các giao dịch kể cả khi Khách Hàng không giao kết các giao dịch đó. Các Điều khoản và Điều kiện này quy định và giải thích các trách nhiệm và nghĩa vụ của Khách Hàng liên quan tới các dịch vụ và thông tin mà Khách Hàng sử dụng hoặc được Ngân Hàng yêu cầu hoặc dịch vụ và thông tin mà Ngân Hàng cung cấp cho Khách Hàng thông qua Ngân hàng Trực tuyến Cá nhân thuộc dịch vụ Ngân hàng Trực tuyến của HSBC.
1. VỀ BẢN CHẤP THUẬN NÀY	**1. VỀ BẢN CHẤP THUẬN NÀY**
N/A	"**Digital Secure Key**" hoặc "**Tính năng Digital Secure Key**" có nghĩa là một tính năng bảo mật hoạt động trên Ứng dụng HSBC Việt Nam, tính năng này được thiết kế để sử dụng cho việc khởi tạo Mã Bảo mật (các Mật khẩu sử dụng một lần) để truy cập và giao dịch qua các dịch vụ Ngân hàng Trực tuyến Cá nhân.

N/A	"**Ứng dụng HSBC Việt Nam**" hoặc "**Ứng dụng ngân hàng di động HSBC Việt Nam**" có nghĩa là ứng dụng di động được cung cấp và cập nhật liên tục bởi Ngân hàng, có thể được tải về trên bất kỳ thiết bị di động nào chạy những hệ điều hành được Ngân Hàng hỗ trợ theo từng thời điểm, mà thông qua ứng dụng đó Khách hàng có thể truy cập các dịch vụ ngân hàng khả dụng trên ứng dụng của Ngân Hàng. Việc sử dụng ứng dụng HSBC Việt Nam tuân thủ theo Điều khoản và Điều kiện sử dụng ứng dụng HSBC Mobile Banking.
N/A	"**Thiết bị di động**" có nghĩa là một thiết bị di động thông minh, bao gồm điện thoại thông minh (Smartphone), máy tính bảng (Tablet), …)
N/A	"**Thiết bị di động được hỗ trợ**" hoặc "**Thiết bị di động tương thích**" có nghĩa là một thiết bị di động thông minh sử dụng những hệ điều hành được Ngân hàng hỗ trợ để có thể cài đặt ứng dụng HSBC Việt Nam.
"**Mã Bảo mật**" có nghĩa là mật khẩu sử dụng một lần được khởi tạo bởi Thiết bị Bảo mật	**"Mã Bảo mật"** có nghĩa là mật khẩu sử dụng một lần được khởi tạo bởi Thiết Bị Bảo Mật hoặc Digital Secure Key.
N/A	"**Phương thức khởi tạo mã bảo mật**" có nghĩa là cách thức và phương pháp tiến hành khởi tạo Mã Bảo mật bằng cách sử dụng Thiết Bị Bảo Mật hoặc Digital Secure Key.
"Tài khoản" có nghĩa là các tài khoản Ngân Hàng gắn liền với Tên đăng nhập, Mật khẩu (nếu áp dụng), và Thiết bị Bảo mật đã được cung cấp cho Khách hàng để sử dụng dịch vụ.	**"Tài khoản"** có nghĩa là các tài khoản Ngân Hàng gắn liền với Tên đăng nhập, Mật khẩu (nếu áp dụng), và Thiết Bị Bảo Mật đã được cung cấp cho Khách Hàng để sử dụng dịch vụ hoặc Digital Secure Key mà Khách Hàng đã kích hoạt thành công để thay thế Thiết Bị Bảo Mật.

3. NGHĨA VỤ BẢO MẬT CỦA KHÁCH HÀNG	3. NGHĨA VỤ BẢO MẬT CỦA KHÁCH HÀNG
b. Để sử dụng các dịch vụ, Khách Hàng sẽ cần một nhận dạng riêng (Tên đăng nhập), một thiết bị bảo mật (Thiết Bị Bảo Mật) và, nếu được yêu cầu, một Mật khẩu.	b. Để sử dụng các dịch vụ, Khách Hàng sẽ cần một nhận dạng riêng (Tên đăng nhập), một Thiết Bị Bảo Mật hoặc Thiết bị di động đã cài Ứng dụng HSBC Việt Nam với tính năng Digital Secure Key đang hoạt động và, nếu được yêu cầu, một Mật khẩu.
N/A	c. Khách hàng là người duy nhất có trách nhiệm cân nhắc kỹ lưỡng và lựa chọn Thiết Bị Bảo Mật/ Digital Secure Key sao cho phù hợp với nhu cầu sử dụng của mình. Mỗi tài khoản Ngân hàng Trực tuyến Cá nhân gắn liền với một Tên tài khoản chỉ được quyền sử dụng duy nhất một phương thức khởi tạo mã bảo mật tại một thời điểm.
N/A	e. Khách hàng là người duy nhất có trách nhiệm kích hoạt tính năng Digital Secure Key để thay thế Thiết Bị Bảo Mật trong việc khởi tạo mã bảo mật
f. Để Thiết lập lại Mật khẩu Trực tuyến, Khách hàng cần cung cấp cho Ngân Hàng Tên đăng nhập, hoàn thành các Câu hỏi để Thiết lập lại Mật khẩu và cung cấp xác nhận sử dụng Thiết bị Bảo mật.	h. Để Thiết lập lại Mật khẩu Trực tuyến, Khách Hàng cần cung cấp cho Ngân Hàng Tên đăng nhập, hoàn thành các Câu hỏi để Thiết lập lại Mật khẩu và cung cấp xác nhận sử dụng Thiết Bị Bảo Mật/ Digital Secure Key.
h. Khách hàng phải giữ bí mật Mật khẩu của mình và bảo mật cho Mật khẩu đó và thực hiện các biện pháp hợp lý để ngăn chặn việc sử dụng trái phép Tên đăng nhập, Mật khẩu, Câu hỏi để Thiết lập lại Mật khẩu và Mã Bảo mật của Khách hàng. Khách hàng không được để người khác chiếm hữu hoặc điều khiển Thiết bị Bảo mật trong bất kì tình huống nào và vào bất kì thời điểm nào.	j. Khách Hàng phải giữ bí mật Mật khẩu của mình và bảo mật cho Mật khẩu đó và thực hiện các biện pháp hợp lý để ngăn chặn việc sử dụng trái phép Tên đăng nhập, Mật khẩu, Câu hỏi để Thiết lập lại Mật khẩu và Mã Bảo mật của Khách Hàng. Khách Hàng không được để người khác chiếm hữu hoặc điều khiển Thiết Bị Bảo Mật hoặc Thiết bị di động được dùng để sử dụng tính năng Digital Secure Key trong bất kì tình huống nào và vào bất kì thời điểm nào.

k. Khách hàng phải thông báo cho Ngân Hàng ngay lập tức về bất kì việc kết nối trái phép nào vào các dịch vụ hoặc về bất kì giao dịch hoặc yêu cầu trái phép nào mà Khách hàng biết hoặc nghi ngờ hoặc nếu Khách hàng nghi ngờ ai đó biết Tên đăng nhập, Mật khẩu, Câu hỏi để Thiết lập lại Mật khẩu và Mã Bảo mật hoặc chiếm hữu, điều khiển hoặc sử dụng Thiết bị Bảo mật.	l. Khách Hàng phải thông báo cho Ngân Hàng ngay lập tức về bất kì việc kết nối trái phép nào vào các dịch vụ hoặc về bất kì giao dịch hoặc yêu cầu trái phép nào mà Khách Hàng biết hoặc nghi ngờ hoặc nếu Khách Hàng nghi ngờ ai đó biết Tên đăng nhập, Mật khẩu, Câu hỏi để Thiết lập lại Mật khẩu và Mã Bảo mật hoặc chiếm hữu, điều khiển hoặc sử dụng Thiết Bị Bảo Mật hoặc Thiết bị di động được dùng để sử dụng tính năng Digital Secure Key.
6. CẤM SỬ DỤNG DỊCH VỤ	**6. CẤM SỬ DỤNG DỊCH VỤ**
b. Khách hàng không được (và không được cố gắng) phá rối hoặc quấy nhiễu dưới bất kì hình thức nào bất kì một phần nào của các dịch vụ (bao gồm trang mạng trực tuyến, Thiết bị Bảo mật hay phần mềm liên quan tới Ngân Hàng hoặc các dịch vụ). Khách hàng không được (và không được cố gắng) kết nối vào bất kì thứ gì liên quan tới các dịch vụ (bao gồm trang mạng trực tuyến hay phần mềm liên quan tới Ngân Hàng hoặc các dịch vụ mà Ngân Hàng không định để Khách hàng kết nối) bao gồm bất kì thứ gì được bảo vệ, trừ khi sử dụng Tên đăng nhập, Mã Bảo mật, Mật Khẩu (nếu áp dụng) và Câu hỏi để Thiết lập lại Mật khẩu.	b. Khách Hàng không được (và không được cố gắng) phá rối hoặc quấy nhiễu dưới bất kì hình thức nào bất kì một phần nào của các dịch vụ (bao gồm trang mạng trực tuyến, Thiết Bị Bảo Mật, Ứng dụng HSBC Việt Nam, tính năng Digital Secure Key hay phần mềm liên quan tới Ngân Hàng hoặc các dịch vụ). Khách Hàng không được (và không được cố gắng) kết nối vào bất kì thứ gì liên quan tới các dịch vụ (bao gồm trang mạng trực tuyến hay phần mềm liên quan tới Ngân Hàng hoặc các dịch vụ mà Ngân Hàng không định để Khách Hàng kết nối) bao gồm bất kì thứ gì được bảo vệ, trừ khi sử dụng Tên đăng nhập, Mã Bảo mật, Mật Khẩu (nếu áp dụng) và Câu hỏi để Thiết lập lại Mật khẩu.
10. TRÁCH NHIỆM CỦA KHÁCH HÀNG ĐỐI VỚI CÁC GIAO DỊCH KHÔNG ĐÚNG THẨM QUYỀN	**10. TRÁCH NHIỆM CỦA KHÁCH HÀNG ĐỐI VỚI CÁC GIAO DỊCH KHÔNG ĐÚNG THẨM QUYỀN**
b. Nếu Khách hàng để bất kì người nào sử dụng một hay nhiều những mục sau: i) Tên đăng nhập, ii) Mật khẩu, iii) Các Câu hỏi để Thiết lập lại Mật khẩu, iv) Thiết bị Bảo mật và/hoặc v) Mã Bảo mật của	b. Nếu Khách Hàng để bất kì người nào sử dụng một hay nhiều những mục sau: i) Tên đăng nhập, ii) Mật khẩu, iii) Các Câu hỏi để Thiết lập lại Mật khẩu, iv) Thiết Bị Bảo Mật/ Digital Secure Key và/hoặc

Khách hàng thì Khách hàng sẽ phải chịu trách nhiệm đối với tất cả các khiếu nại, tổn thất và hậu quả phát sinh từ hoặc liên quan tới tất cả các giao dịch được tiến hành thông qua việc sử dụng các dịch vụ bởi hoặc với sự đồng ý của người đó.	v) Mã Bảo mật của Khách Hàng thì Khách Hàng sẽ phải chịu trách nhiệm đối với tất cả các khiếu nại, tổn thất và hậu quả phát sinh từ hoặc liên quan tới tất cả các giao dịch được tiến hành thông qua việc sử dụng các dịch vụ bởi hoặc với sự đồng ý của người đó.
c. Nếu Khách hàng có tham gia vào một giao dịch không đúng thẩm quyền, Khách hàng sẽ phải chịu trách nhiệm về một số hoặc tất cả các tổn thất phát sinh từ giao dịch không đúng thẩm quyền đó. Các cách mà Khách hàng tham gia vào một giao dịch không đúng thẩm quyền bao gồm cả việc không thực hiện các bước hợp lý để theo dõi bất kì nghĩa vụ bảo mật nào được đề cập đến trong các Điều khoản này và/hoặc bất kì một sự chậm trễ không chính đáng nào trong việc thông báo cho Ngân Hàng về việc tiết lộ hoặc khả năng tiết lộ cho người khác Tên đăng nhập hoặc Mật khẩu hoặc các Câu hỏi để Thiết lập lại Mật khẩu hoặc Mã Bảo mật và/hoặc việc sử dụng, điều khiển không đúng thẩm quyền hoặc mất Thiết bị Bảo mật của Khách hàng.	c. Nếu Khách Hàng có tham gia vào một giao dịch không đúng thẩm quyền, Khách Hàng sẽ phải chịu trách nhiệm về một số hoặc tất cả các tổn thất phát sinh từ giao dịch không đúng thẩm quyền đó. Các cách mà Khách Hàng tham gia vào một giao dịch không đúng thẩm quyền bao gồm cả việc không thực hiện các bước hợp lý để theo dõi bất kì nghĩa vụ bảo mật nào được đề cập đến trong các Điều khoản này và/hoặc bất kì một sự chậm trễ không chính đáng nào trong việc thông báo cho Ngân Hàng về việc tiết lộ hoặc khả năng tiết lộ cho người khác Tên đăng nhập hoặc Mật khẩu hoặc các Câu hỏi để Thiết lập lại Mật khẩu hoặc Mã Bảo mật và/hoặc việc sử dụng, điều khiển không đúng thẩm quyền hoặc mất Thiết Bị Bảo Mật/ Thiết bị di động được dùng để sử dụng Tính năng Digital Secure Key của Khách Hàng.
d. Nếu Khách hàng đã thông báo sớm trong khả năng có thể cho Ngân Hàng về việc tiết lộ hoặc khả năng tiết lộ cho người khác Tên đăng nhập hoặc Mật khẩu hoặc các Câu hỏi để Thiết lập lại Mật khẩu hoặc Mã Bảo mật và/hoặc việc sử dụng, điều khiển không đúng thẩm quyền hoặc mất Thiết bị Bảo mật của Khách hàng thì Khách hàng sẽ không phải chịu trách nhiệm đối với các tổn thất phát sinh sau khi Ngân Hàng đã nhận được thông báo đó trừ khi Khách Hàng hành động một cách cố ý hoặc bất cẩn.	d. Nếu Khách Hàng đã thông báo sớm trong khả năng có thể cho Ngân Hàng về việc tiết lộ hoặc khả năng tiết lộ cho người khác Tên đăng nhập hoặc Mật khẩu hoặc các Câu hỏi để Thiết lập lại Mật khẩu hoặc Mã Bảo mật và/hoặc việc sử dụng, điều khiển không đúng thẩm quyền hoặc mất Thiết Bị Bảo Mật/ Thiết bị di động được dùng để sử dụng Tính năng Digital Secure Key của Khách Hàng thì Khách Hàng sẽ không phải chịu trách nhiệm đối với các tổn thất

	phát sinh sau khi Ngân Hàng đã nhận được thông báo đó trừ khi Khách Hàng hành động một cách cố ý hoặc bất cẩn.
11. THIẾT BỊ BẢO MẬT	**11. THIẾT BỊ BẢO MẬT/ DIGITAL SECURE KEY**
Ngân Hàng sẽ nỗ lực hợp lí để bảo đảm rằng Thiết bị Bảo mật đã cung cấp cho Khách hàng sẽ hoạt động ở mức cần thiết để cho phép kết nối với các dịch vụ khi được yêu cầu. Khách hàng phải thông báo cho Ngân Hàng ngay lập tức nếu bất kì Thiết bị Bảo mật nào không hoạt động đúng chức năng và nghĩa vụ duy nhất của Ngân Hàng đối với Thiết bị Bảo mật đó là thay thế nó bởi một Thiết bị Bảo mật mới với mức phí mà Ngân Hàng sẽ quy định tùy từng thời điểm, ngoại trừ trong các trường hợp dưới đây: a. Thiết bị Bảo mật có lỗi được chuyển trả cho Ngân Hàng trong vòng 90 ngày kể từ ngày được cấp; và b. Ngân Hàng có bằng chứng là Khách hàng không có lỗi hoặc bất cẩn dẫn đến hoặc góp phần làm cho Thiết bị Bảo mật không hoạt động đúng chức năng. Trừ những điều quy định trong Khoản 11(a) này, Ngân Hàng sẽ không chịu trách nhiệm liên quan tới Thiết bị Bảo mật, bao gồm cả trách nhiệm đối với việc vi phạm bất kì điều khoản ngụ ý nào về chất lượng phù hợp, sự vận hành hay sự thích hợp cho một mục đích nào đó của bất kì Thiết bị Bảo mật nào. Ngoài ra, Ngân hàng không thể chịu trách nhiệm về bất kì mất mát hay tổn thất nào mà Khách hàng gặp phải hay phải gánh chịu do việc Khách hàng không giữ bảo mật và/hoặc không sử dụng Thiết bị Bảo mật đúng theo Yêu cầu và khuyến cáo của Ngân Hàng.	a. Ngân Hàng sẽ nỗ lực hợp lí để bảo đảm rằng Thiết bị Bảo mật đã cung cấp cho Khách hàng sẽ hoạt động ở mức cần thiết để cho phép kết nối với các dịch vụ khi được yêu cầu. b. Khách hàng phải thông báo cho Ngân Hàng ngay lập tức nếu bất kì Thiết bị Bảo mật nào không hoạt động đúng chức năng và nghĩa vụ duy nhất của Ngân Hàng đối với Thiết bị Bảo mật đó là thay thế nó bởi một Thiết bị Bảo mật mới với mức phí mà Ngân Hàng sẽ quy định tùy từng thời điểm, ngoại trừ trong các trường hợp dưới đây: i) Thiết bị Bảo mật có lỗi được chuyển trả cho Ngân Hàng trong vòng 90 ngày kể từ ngày được cấp; và ii) Ngân Hàng có bằng chứng là Khách hàng không có lỗi hoặc bất cẩn dẫn đến hoặc góp phần làm cho Thiết bị Bảo mật không hoạt động đúng chức năng. Trừ những điều quy định trong Khoản 11(a) này, Ngân Hàng sẽ không chịu trách nhiệm liên quan tới Thiết bị Bảo mật, bao gồm cả trách nhiệm đối với việc vi phạm bất kì điều khoản ngụ ý nào về chất lượng phù hợp, sự vận hành hay sự thích hợp cho một mục đích nào đó của bất kì Thiết bị Bảo mật nào. Ngoài ra, Ngân hàng không thể chịu trách nhiệm về bất kì mất mát hay tổn thất nào mà Khách hàng gặp phải hay phải gánh chịu

	do việc Khách hàng không giữ bảo mật và/hoặc không sử dụng Thiết bị Bảo mật đúng theo Yêu cầu và khuyến cáo của Ngân Hàng.
N/A	c. Từ tháng 02 năm 2021, trừ trường hợp Ngân hàng có quyết định khác, tính năng Digital Secure Key là công cụ mặc định (thay thế Thiết Bị Bảo Mật) để tạo Mã bảo mật cho Ngân hàng Trực tuyến Cá nhân. i) Đối với Khách hàng hiện đang sử dụng Thiết Bị Bảo Mật, khi Khách hàng kích hoạt thành công tính năng Digital Secure Key, Thiết Bị Bảo Mật của Khách hàng sẽ lập tức bị mất hiệu lực sử dụng. ii) Khách hàng có thể trì hoãn việc kích hoạt Digital Secure Key trong một khoảng thời gian nhất định ("Thời gian chờ") được quy định cụ thể bởi Ngân hàng tại từng thời điểm. Trong khoảng Thời gian chờ, Khách hàng vẫn có thể sử dụng Thiết Bị Bảo Mật và Ứng dụng HSBC Việt Nam bình thường. iii) Sau Thời gian chờ, nếu Khách hàng vẫn chưa kích hoạt thành công tính năng Digital Secure Key, Khách hàng vẫn có thể tiếp tục sử dụng Thiết Bị Bảo Mật để đăng nhập và sử dụng các dịch vụ khả dụng trên Ngân hàng Trực tuyến Cá nhân, tuy nhiên Khách hàng sẽ không thể truy cập và sử dụng Ứng dụng HSBC Việt Nam cho đến khi Khách hàng kích hoạt thành công tính năng Digital Secure Key.

	iv) Trong trường hợp khách hàng đã kích hoạt Digital Secure Key để sử dụng nhưng sau đó muốn quay về sử dụng Thiết Bị Bảo Mật, với điều kiện Thiết Bị Bảo Mật vẫn tiếp tục được cung cấp/chấp nhận bởi Ngân hàng, Khách hàng sẽ phải tuân theo quy trình của Ngân hàng tại thời điểm đó cho việc thay đổi phương thức tạo mã bảo mật, và chịu mọi khoản phí có thể được áp dụng. v) Khi có bất kỳ thiết bị di động nào của Khách hàng dùng để sử dụng tính năng Digital Secure Key trở nên không thể vận hành bình thường các tính năng cần thiết, bị suy giảm mức độ bảo mật hoặc không thể duy trì việc tuân thủ yêu cầu bảo mật theo hướng dẫn/khuyến nghị của Ngân hàng, hoặc không còn nằm trong quyền kiểm soát của Khách hàng (dù là vô tính hay cố ý) bao gồm (nhưng không giới hạn) các trường hợp như: hư hại, bị thất lạc, mất cắp, thay đổi, bị tấn công can thiệp quyền kiểm soát hoặc đánh cắp dữ liệu, … Khách hàng có trách nhiệm ngay lập tức tự gỡ thiết bị đó khỏi danh sách thiết bị được đăng ký sử dụng Ứng dụng HSBC Việt Nam thông qua: (i) Ứng dụng HSBC Việt nam được cài đặt trên một thiết bị di động tương thích khác (tuỳ vào tình trạng khả dụng của tính năng liên quan trên Ứng dụng HSBC Việt Nam tại từng thời điểm); (ii) liên hệ Trung tâm Dịch vụ Khách hàng của Ngân hàng; hoặc (iii) bất kỳ phương thức nào khác được Ngân hàng áp dụng tại từng thời điểm.

16. CÁC VẤN ĐỀ CHUNG	16. CÁC VẤN ĐỀ CHUNG
c. Bồi hoàn: Bằng việc kết nối, sử dụng và/hoặc tiếp tục sử dụng Trang mạng của các dịch vụ này, Khách Hàng thể hiện sự đồng ý sẽ bồi hoàn và bảo đảm cho HSBC, giám đốc, nhân viên, người được chỉ định và đại diện của HSBC được bồi hoàn đối với tất cả các hành động, trách nhiệm, chi phí, khiếu nại, mất mát, tổn thất, kiện cáo và/hoặc các khoản phí (bao gồm tất cả các chi phí luật sư trên cơ sở khoản bồi hoàn) mà Ngân Hàng phải gánh chịu hoặc gặp phải bao gồm nhưng không giới hạn, liên quan tới hoặc phát sinh từ: ii) Bất kì yêu cầu không đúng thẩm quyền nào (bao gồm Yêu cầu từ người không có quyền và/hoặc yêu cầu được đưa ra từ việc sử dụng không đúng thẩm quyền Tên đăng nhập Mật khẩu (nếu áp dụng), các Câu hỏi để Thiết lập lại Mật khẩu và/hoặc Mã Bảo mật và/hoặc Thiết Bị Bảo Mật) có thể được truyền qua Ngân hàng Trực tuyến Cá nhân hoặc bất kì yêu cầu không đầy đủ, không chính xác hoặc sai lạc nào; iv) Bất kì vi phạm hoặc việc không tuân thủ bất kì Điều khoản nào của Khách Hàng hoặc của bất kì người không có thẩm quyền nào sử dụng Tên đăng nhập/Mã cá nhân Ngân Hàng Trực tuyến, Mật khẩu, các Câu hỏi để Thiết lập lại Mật khẩu và Thiết Bị Bảo Mật của Khách Hàng;	c. Bồi hoàn: Bằng việc kết nối, sử dụng và/hoặc tiếp tục sử dụng Trang mạng của các dịch vụ này, Khách Hàng thể hiện sự đồng ý sẽ bồi hoàn và bảo đảm cho HSBC, giám đốc, nhân viên, người được chỉ định và đại diện của HSBC được bồi hoàn đối với tất cả các hành động, trách nhiệm, chi phí, khiếu nại, mất mát, tổn thất, kiện cáo và/hoặc các khoản phí (bao gồm tất cả các chi phí luật sư trên cơ sở khoản bồi hoàn) mà Ngân Hàng phải gánh chịu hoặc gặp phải bao gồm nhưng không giới hạn, liên quan tới hoặc phát sinh từ: ii) Bất kì yêu cầu không đúng thẩm quyền nào (bao gồm Yêu cầu từ người không có quyền và/hoặc yêu cầu được đưa ra từ việc sử dụng không đúng thẩm quyền Tên đăng nhập Mật khẩu (nếu áp dụng), các Câu hỏi để Thiết lập lại Mật khẩu và/hoặc Mã Bảo mật và/hoặc Thiết Bị Bảo Mật/ Digital Secure Key) có thể được truyền qua Ngân hàng Trực tuyến Cá nhân hoặc bất kì yêu cầu không đầy đủ, không chính xác hoặc sai lạc nào; iv) Bất kì vi phạm hoặc việc không tuân thủ bất kì Điều khoản nào của Khách Hàng hoặc của bất kì người không có thẩm quyền nào sử dụng Tên đăng nhập/Mã cá nhân Ngân Hàng Trực tuyến, Mật khẩu, các Câu hỏi để Thiết lập lại Mật khẩu và Thiết Bị Bảo Mật/ Digital Secure Key của Khách Hàng;

CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN SỬ DỤNG DỊCH VỤ NGÂN HÀNG QUA ĐIỆN THOẠI HIỆN TẠI	CÁC ĐIỀU KHOẢN VÀ ĐIỀU KIỆN SỬ DỤNG DỊCH VỤ NGÂN HÀNG QUA ĐIỆN THOẠI
3. HOẠT ĐỘNG CỦA DỊCH VỤ NGÂN HÀNG QUA ĐIỆN THOẠI	**3. HOẠT ĐỘNG CỦA DỊCH VỤ NGÂN HÀNG QUA ĐIỆN THOẠI**
Khách Hàng có thể sử dụng Dịch Vụ Ngân Hàng Qua Điện Thoại để: (a) kiểm tra số dư của các Tài Khoản; (b) lấy thông tin về những giao dịch vừa được thực hiện trên Tài Khoản; (c) chuyển tiền từ Tài Khoản Chỉ Định qua Tài Khoản Thẻ Tín Dụng của Khách Hàng nêu trong Dịch Vụ Ngân Hàng Qua Điện Thoại đã được xác định trước về giới hạn chỉ định chuyển khoản; (d) lấy thông tin về các tỷ giá ngoại hối và lãi suất tiền gửi; (e) kích hoạt Thẻ Tín Dụng, bao gồm việc kích hoạt thẻ qua Trung Tâm Dịch Vụ Khách Hàng, Dịch Vụ Ngân Hàng tự động Qua Điện Thoại hoặc tin nhắn SMS theo quy định của Ngân Hàng quy định; (f) tiến hành các dịch vụ ngân hàng và dịch vụ thẻ tín dụng khác mà Ngân Hàng sẽ giới thiệu tại từng thời điểm.	Khách Hàng có thể sử dụng Dịch Vụ Ngân Hàng Qua Điện Thoại để: (a) kiểm tra số dư của các Tài Khoản; (b) lấy thông tin về những giao dịch vừa được thực hiện trên Tài Khoản; (c) chuyển tiền từ Tài Khoản Chỉ Định qua Tài Khoản Thẻ Tín Dụng của Khách Hàng nêu trong Dịch Vụ Ngân Hàng Qua Điện Thoại đã được xác định trước về giới hạn chỉ định chuyển khoản; (d) kích hoạt Thẻ Tín Dụng; Hàng tự động Qua Điện Thoại hoặc tin nhắn SMS theo quy định của Ngân Hàng quy định; (e) tiến hành các dịch vụ ngân hàng và dịch vụ thẻ tín dụng khác mà Ngân Hàng sẽ giới thiệu tại từng thời điểm.

SUMMARY OF CHANGES ABOUT TERMS & CONDITIONS

(This amendment is effective from 24 Feb 2021)

A. Personal Banking Customer

Current Terms and Conditions	Terms and Conditions effective on 24 Feb 2021
***Note:** Contents which are not included in current Terms and Conditions are marked as N/A*	***Note:** Revised contents are marked in red*
GENERAL TERMS AND CONDITIONS	**GENERAL TERMS AND CONDITIONS**
5. TRANSACTION RECORD AND NOTIFICATION 5.8. The Customer warrants that all particulars given to the Bank (whether in an Account Opening Form or otherwise) are, to the best of the Customer's knowledge, accurate and updated. The Customer undertakes to notify the Bank of any changes to these particulars, including but not limited to that the Customer must notify the Bank without delay of any changes in the Customer's, Account Holder's name and address, as well as the termination of, or amendment to, any powers of representation towards the Bank conferred on any person. The Customer hereby authorizes and agrees, for the Bank to update Customer's resident status based on information/ documents provided by Customers, by the way that the Bank deems appropriate.	**5. TRANSACTION RECORD AND NOTIFICATION** 5.8. The Customer warrants that all particulars given to the Bank (whether in an Account Opening Form or otherwise) are, to the best of the Customer's knowledge, accurate and updated. The Customer undertakes to notify the Bank of any changes to these particulars, including but not limited to that the Customer must notify the Bank without delay of any changes in the Customer's, Account Holder's name and address, as well as the termination of, or amendment to, any powers of representation towards the Bank conferred on any person. The Customer hereby authorizes and agrees, for the Bank to update Customer's resident status and other information of Customers (full name, date of birth, ID/Passport with place/date of issuance, address) based on information/ documents provided by Customers, by the way that the Bank deems appropriate without additional acceptance request from Customers. This update might also include abbreviation or

	mismatched information between documents provided by the customer and customers' Instructions. The decision is based on documents in line with the Bank's policy.
INTERNET BANKING TERMS AND CONDITIONS	**INTERNET BANKING TERMS AND CONDITIONS**
IMPORTANT! Please note carefully your security duties set out in Clauses 3 and 10 below. If you breach any of your security duties you may be liable for the transactions even if you did not authorize them. These Terms and Conditions explain your responsibilities and obligations relating to services and information that you use or request from us, or we provide you, through HSBC's Internet Banking service, Personal Internet Banking.	**IMPORTANT!** Please note carefully the Internet Banking Terms and Conditions, especially your security duties set out in Clauses 3 and 10 below. If you breach any of your security duties you may be liable for the transactions even if you did not authorize them. These Terms and Conditions provide and explain your responsibilities and obligations relating to services and information that you use or request from us, or we provide you, through HSBC's Internet Banking service, Personal Internet Banking.
1. ABOUT THIS CONTRACT	**1. ABOUT THIS CONTRACT**
N/A	"**Digital Secure Key**" or "**Digital Secure Key feature**" means a security feature available on HSBC Vietnam app, designed to be used to generate Security Code (one-time passwords) to access and use Personal Internet Banking services.
N/A	"**HSBC Vietnam app**" or "**HSBC Vietnam mobile banking app**" means an application provided and updated from time to time by the Bank which can be downloaded to any mobile device using operating systems supported by the Bank from time to time, via which customer can access banking services available on the application. The use of HSBC Vietnam app subject to HSBC Mobile Banking App Terms and Conditions.

N/A	"**Mobile device**" means any smart mobile device including Smartphone, Tablet, etc.
N/A	"**Supported mobile device**" or "**Compatible mobile device**" means any mobile device using any operating system (OS) supported by the Bank to be able to set up the HSBC Vietnam app.
"Security Code" means a one-time password generated by the Security Device.	**"Security Code"** means a one-time password generated by the Security Device or Digital Secure Key.
N/A	"**Security code generating method**" means a method to generate a Security code using Security Device or Digital Secure Key.
"Account" means the bank accounts with us that are associated with the Username, Password (if applicable), and Security Device issued to you for the services.	**"Account"** means the bank accounts with us that are associated with the Username, Password (if applicable), and Security Device issued to you for the services or activated Digital Secure Key replacing Security Device;
3. YOUR SECURITY DUTIES	**3. YOUR SECURITY DUTIES**
b. To use the services, you will need a unique identifier (Username), and a Security Device and, if required, a Password.	b. To use the services, you will need a unique identifier (Username), and a Security Device/ Digital Secure Key and, if required, a Password.
N/A	c. It is your sole responsibility to consider carefully and choose either Digital Secure Key or Security Device which is suitable to your needs. Each Personal Internet Banking account is connected with only one security code generating method at a time.
N/A	e. It is your sole responsibility to activate the Digital Secure Key to replace your Security Device to generate a security code.

f. To reset your password online (OLR), you need to provide us with your Username, complete the Password Reset Questions, and provide authentication using the Security Device.	h. To reset your password online (OLR), you need to provide us with your Username, complete the Password Reset Questions, and provide authentication using the Security Device/ Digital Secure Key.
h. You must keep your Password secret and secure at all times and exercise reasonable care and diligence to prevent unauthorised use of your Username, Password, Password Reset Questions, Security Device and Security Code. At no time and under no circumstances shall you permit the Security Device to come into the possession or control of any other person(s).	j. You must keep your Password secret and secure at all times and exercise reasonable care and diligence to prevent unauthorised use of your Username, Password, Password Reset Questions, Security Device/ Mobile device on which Digital Secure Key is used and Security Code. At no time and under no circumstances shall you permit the Security Device to come into the possession or control of any other person(s).
j. You must notify us immediately of any unauthorised access to the services or any unauthorized transaction or instruction that you know of or suspect or if you suspect someone else knows your Username, Password, Password Reset Questions, Security Code or has unauthorised possession, control or use of your Security Device.	l. You must notify us immediately of any unauthorised access to the services or any unauthorized transaction or instruction that you know of or suspect or if you suspect someone else knows your Username, Password, Password Reset Questions, Security Code or has unauthorised possession, control or use of your Security Device/ Mobile device on which Digital Secure Key is used.
6. PROHIBITED USES OF THE SERVICES	**6. PROHIBITED USES OF THE SERVICES**
b. You must not (and must not attempt to) tamper or interfere in any way with any part of the services (including any internet site, Security Device or any software relating to us or services). You must not (and must not attempt to) access anything relating to the services (including any internet site or any software relating to us or the services that we do not intend you to access), including	b. You must not (and must not attempt to) tamper or interfere in any way with any part of the services (including any internet site, Security Device, HSBC Vietnam application, Digital Secure Key feature or any software relating to us or services). You must not (and must not attempt to) access anything relating to the services (including any internet site or any software relating to us or the

anything protected, except with your Username, Security Code, Password Reset Questions and, if applicable, Password.	services that we do not intend you to access), including anything protected, except with your Username, Security Code, Password Reset Questions and, if applicable, Password.
10. YOUR LIABILITY FOR UNAUTHORISED TRANSACTIONS	**10. YOUR LIABILITY FOR UNAUTHORISED TRANSACTIONS**
b. If you let any other person use any one or more of the following: i) your Username, ii) your Password, iii) Password Reset Questions, iv) your Security Device and/or v) your Security Code; you are liable for all claims, losses and consequences arising from or in connection with all transactions made using the services by or with the consent of that person.	b. If you let any other person use any one or more of the following: i) your Username, ii) your Password, iii) Password Reset Questions, iv) your Security Device/ Digital Secure Key and/or v) your Security Code; you are liable for all claims, losses and consequences arising from or in connection with all transactions made using the services by or with the consent of that person.
c. If you have contributed to an unauthorised transaction, you may be liable for some or all of the loss resulting from the unauthorised transaction. Ways you can contribute to an unauthorized transaction include, but are not limited to, failing to take reasonable steps to observe any of your security duties referred to in these Terms and/or any unreasonable delay in notifying us of an actual or possible disclosure to any other person of your Username or Password or Password Reset Questions or Security Code and/or unauthorised use, control or loss of your Security Device.	c. If you have contributed to an unauthorised transaction, you may be liable for some or all of the loss resulting from the unauthorised transaction. Ways you can contribute to an unauthorized transaction include, but are not limited to, failing to take reasonable steps to observe any of your security duties referred to in these Terms and/or any unreasonable delay in notifying us of an actual or possible disclosure to any other person of your Username or Password or Password Reset Questions or Security Code and/or unauthorised use, control or loss of your Security Device/ Mobile device on which Digital Secure Key is used.
If you have reported the following as soon as reasonably practicable an actual or possible disclosure of your Username or Password or Password Reset Questions or Security Code and/or unauthorised use, control or loss of your Security Device. to us, and HSBC has received this report, you will	d. If you have reported the following as soon as reasonably practicable an actual or possible disclosure of your Username or Password or Password Reset Questions or Security Code and/or unauthorised use, control or loss of your Security Device/ Mobile

not be liable for the loss incurred after HSBC has received this report unless you have acted fraudulently or negligently.	device on which Digital Secure Key is used. to us, and HSBC has received this report, you will not be liable for the loss incurred after HSBC has received this report unless you have acted fraudulently or negligently.
11. SECURITY DEVICE/ DIGITAL SECURE KEY	**11. SECURITY DEVICE/ DIGITAL SECURE KEY**
We will make all reasonable efforts to ensure that the Security Device provided to you will perform as necessary to permit access to the services as and when required. You must notify us immediately if any Security Device fails to function correctly and the only obligations that we have in respect of such Security Device is to replace the same with a new Security Device for a fee which we shall determine the rate at our discretion from time to time, except under the following conditions: a. Upon the defective Security Device being returned to us within 90 days of its date of issue; and b. If we are satisfied that there is no default or negligence on your part which results in or contributes to the Security Device's failure to function correctly. Other than as specified in this Clause 11(a), we shall have no other liability in relation to this Security Device including, without limitation, liability for breach of any implied term as to satisfactory quality, merchantability or fitness for purpose of any Security Device. In addition, we cannot be held liable for any loss or damages incurred or suffered by you arising from your failure to safe-keep and/or use the Security Device in accordance with our instructions and recommendations.	a. We will make all reasonable efforts to ensure that the Security Device/ Digital Secure Key provided to you will perform as necessary to permit access to the services as and when required. b. You must notify us immediately if any Security Device fails to function correctly and the only obligations that we have in respect of such Security Device is to replace the same with a new Security Device for a fee which we shall determine the rate at our discretion from time to time, except under the following conditions: i) Upon the defective Security Device being returned to us within 90 days of its date of issue; and ii) If we are satisfied that there is no default or negligence on your part which results in or contributes to the Security Device's failure to function correctly. Other than as specified in this Clause 11(a), we shall have no other liability in relation to this Security Device including, without limitation, liability for breach of any implied term as to satisfactory quality, merchantability or fitness for purpose of any Security Device. In addition, we cannot be held liable for any loss or damages incurred or suffered by you arising from

	your failure to safe-keep and/or use the Security Device in accordance with our instructions and recommendations.
N/A	c. From February 2021, unless the Bank decides otherwise, Digital Secure Key feature shall be the default instrument (replacing Security Device) to generate Security Code for Personal Internet Banking. i) If you are currently using Security Device, as soon as you succesfully activate Digital Secure Key feature, your Security Device shall be deactivated immediately. ii) You can defer the Digital Secure Key activation within a certain period ("Deferment period") prescribed by us. During this Deferment period, you can still use your Security Device as well as the HSBC Vietnam app as usual. iii) After the Deferment period ends, if you have not successfully activated Digital Secure Key feature, you can still continue to use your Security Device to access and use services available on Personal Internet Banking. However, you cannot use the HSBC Vietnam app until you activate Digital Secure Key successfully. iv) In case you have activated Digital Secure Key successfully but then want to switch back to Security Device, provided that the Security Device is availably provided/accepted by the Bank, you shall have to follow our procedures applied at

	that time for changing Security code generating method as well as bear all the applicable fees and charges (if any). v) When any mobile device of yours on which the Digital Secure Key feature is used (deliberately or undeliberately)become malfunction, has its security compromised or cannot maintain security measures required or recommended by the Bank, or is no longer under your own control, including (but not limited) the following circumstances: broken, damaged, lost, stolen, replaced, hacked, jail-broken or rooted or data compromised, etc., you must immediatly remove that mentioned mobile device from the mobile device list registered for using HSBC Vietnam app via: (i) HSBC Vietnam app installed on another compatible mobile device (depending on the availablility of the relevant features on the HSBC Vietnam app from time to time); (ii) our Contact Center, or (iii) using any other methods provided by the Bank from time to time.
16. GENERAL	**16. GENERAL**
c. Indemnity: By your access, use and/or continued use of these services Website, you signify your agreement to indemnify and to keep indemnified HSBC, its directors, employees, nominees and agents fully against all actions, liabilities, costs, claims, losses, damages, proceedings and/or expenses (including all legal costs on an indemnity basis) suffered or incurred by us including but not limited to, in connection with or arising from:	c. Indemnity: By your access, use and/or continued use of these services Website, you signify your agreement to indemnify and to keep indemnified HSBC, its directors, employees, nominees and agents fully against all actions, liabilities, costs, claims, losses, damages, proceedings and/or expenses (including all legal costs on an indemnity basis) suffered or incurred by us including but not limited to, in connection with or arising from:

ii) any unauthorised instructions (including but not limited to, instructions from unauthorised person(s) and/or instructions transmitted due to unauthorised use of the Username and/or Password, Password Reset Questions and/or Security Code and/or Security Device) that might be transmitted through Personal Internet Banking or any instructions which are incomplete, inaccurate or garbled; iv) any breach or non-observance of any of these Terms by you or by any other unauthorized person(s) using your Username, Password, Password Reset Questions and Security Device;	ii) any unauthorised instructions (including but not limited to, instructions from unauthorised person(s) and/or instructions transmitted due to unauthorised use of the Username and/or Password, Password Reset Questions and/or Security Code and/or Security Device/ Digital Secure Key) that might be transmitted through Personal Internet Banking or any instructions which are incomplete, inaccurate or garbled; iv) any breach or non-observance of any of these Terms by you or by any other unauthorized person(s) using your Username, Password, Password Reset Questions and Security Device/ Digital Secure Key;
CURRENT PHONEBANKING SERVICES TERMS AND CONDITIONS	**PHONEBANKING SERVICES TERMS AND CONDITIONS**
3. OPERATION OF PHONEBANKING SERVICES The Customer may use PhoneBanking Services to: (a) enquire as to the balance of Account; (b) obtain information on recent transactions performed on Account; (c) transfer of funds from the Dedicated Transferor Account to the Credit Card Accounts of the Customer with which the PhoneBanking Services are established within the pre-defined dedicated transfer limits; (d) obtain information on exchange and deposit rates;	**3. OPERATION OF PHONEBANKING SERVICES** The Customer may use PhoneBanking Services to: (a) enquire as to the balance of Account; (b) obtain information on recent transactions performed on Account; (c) transfer of funds from the Dedicated Transferor Account to the Credit Card Accounts of the Customer with which the PhoneBanking Services are established within the pre-defined dedicated transfer limits; (d) activate the Credit Card(s);

(e) activate the Credit Card(s), including the activation via Contact Center, Interactive Voice Record or the SMS as designed by the Bank; (f) perform other types of banking and credit card services as the Bank may from time to time introduce.	(e) perform other types of banking and credit card services as the Bank may from time to time introduce.

B. Premier Customer

Current Terms and Conditions	Terms and Conditions effective on 24 Feb 2021
***Note:** Contents which are not included in current Terms and Conditions are marked as N/A*	***Note:** Revised contents are marked in red*
INTERNET BANKING TERMS AND CONDITIONS	**INTERNET BANKING TERMS AND CONDITIONS**
IMPORTANT! Please note carefully your security duties set out in Clauses 3 and 10 below. If you breach any of your security duties you may be liable for the transactions even if you did not authorize them. These Terms and Conditions explain your responsibilities and obligations relating to services and information that you use or request from us, or we provide you, through HSBC's Internet Banking service, Personal Internet Banking.	**IMPORTANT!** Please note carefully the Internet Banking Terms and Conditions, especially your security duties set out in Clauses 3 and 10 below. If you breach any of your security duties you may be liable for the transactions even if you did not authorize them. These Terms and Conditions provide and explain your responsibilities and obligations relating to services and information that you use or request from us, or we provide you, through HSBC's Internet Banking service, Personal Internet Banking.
1. ABOUT THIS CONTRACT	**1. ABOUT THIS CONTRACT**
N/A	"**Digital Secure Key**" or "**Digital Secure Key feature**" means a security feature available on HSBC Vietnam app, designed to be used to generate Security Code (one-time passwords) to access and use Personal Internet Banking services.
N/A	"**HSBC Vietnam app**" or "**HSBC Vietnam mobile banking app**" means an application provided and updated from time to time by the Bank which can be downloaded to any mobile device using operating systems supported by the Bank from time to time, via which customer can access banking services available on the application. The use of

	HSBC Vietnam app subject to HSBC Mobile Banking App Terms and Conditions.
N/A	"**Mobile device**" means any smart mobile device including Smartphone, Tablet, etc.
N/A	"**Supported mobile device**" or "**Compatible mobile device**" means any mobile device using any operating system (OS) supported by the Bank to be able to set up the HSBC Vietnam app.
"Security Code" means a one-time password generated by the Security Device.	**"Security Code"** means a one-time password generated by the Security Device or Digital Secure Key.
N/A	"**Security code generating method**" means a method to generate a Security code using Security Device or Digital Secure Key.
"Account" means the bank accounts with us that are associated with the Username, Password (if applicable), and Security Device issued to you for the services.	**"Account"** means the bank accounts with us that are associated with the Username, Password (if applicable), and Security Device issued to you for the services or activated Digital Secure Key replacing Security Device;
3. YOUR SECURITY DUTIES	**3. YOUR SECURITY DUTIES**
b. To use the services, you will need a unique identifier (Username), and a Security Device and, if required, a Password.	b. To use the services, you will need a unique identifier (Username), and a Security Device/ Digital Secure Key and, if required, a Password.
N/A	c. It is your sole responsibility to consider carefully and choose either Digital Secure Key or Security Device which is suitable to your needs. Each Personal Internet Banking account is connected with only one security code generating method at a time.

N/A	e. It is your sole responsibility to activate the Digital Secure Key to replace your Security Device to generate a security code.
f. To reset your password online (OLR), you need to provide us with your Username, complete the Password Reset Questions, and provide authentication using the Security Device.	h. To reset your password online (OLR), you need to provide us with your Username, complete the Password Reset Questions, and provide authentication using the Security Device/ Digital Secure Key.
h. You must keep your Password secret and secure at all times and exercise reasonable care and diligence to prevent unauthorised use of your Username, Password, Password Reset Questions, Security Device and Security Code. At no time and under no circumstances shall you permit the Security Device to come into the possession or control of any other person(s).	j. You must keep your Password secret and secure at all times and exercise reasonable care and diligence to prevent unauthorised use of your Username, Password, Password Reset Questions, Security Device/ Mobile device on which Digital Secure Key is used and Security Code. At no time and under no circumstances shall you permit the Security Device to come into the possession or control of any other person(s).
j. You must notify us immediately of any unauthorised access to the services or any unauthorized transaction or instruction that you know of or suspect or if you suspect someone else knows your Username, Password, Password Reset Questions, Security Code or has unauthorised possession, control or use of your Security Device.	l. You must notify us immediately of any unauthorised access to the services or any unauthorized transaction or instruction that you know of or suspect or if you suspect someone else knows your Username, Password, Password Reset Questions, Security Code or has unauthorised possession, control or use of your Security Device/ Mobile device on which Digital Secure Key is used.
6. PROHIBITED USES OF THE SERVICES	**6. PROHIBITED USES OF THE SERVICES**
b. You must not (and must not attempt to) tamper or interfere in any way with any part of the services (including any internet site, Security Device or any software relating to us or services). You must not (and must not attempt to) access anything relating to the	b. You must not (and must not attempt to) tamper or interfere in any way with any part of the services (including any internet site, Security Device, HSBC Vietnam application, Digital Secure Key feature or any software relating to us or services). You must not

services (including any internet site or any software relating to us or the services that we do not intend you to access), including anything protected, except with your Username, Security Code, Password Reset Questions and, if applicable, Password.	(and must not attempt to) access anything relating to the services (including any internet site or any software relating to us or the services that we do not intend you to access), including anything protected, except with your Username, Security Code, Password Reset Questions and, if applicable, Password.
10. YOUR LIABILITY FOR UNAUTHORISED TRANSACTIONS	**10. YOUR LIABILITY FOR UNAUTHORISED TRANSACTIONS**
b. If you let any other person use any one or more of the following: i) your Username, ii) your Password, iii) Password Reset Questions, iv) your Security Device and/or v) your Security Code; you are liable for all claims, losses and consequences arising from or in connection with all transactions made using the services by or with the consent of that person.	b. If you let any other person use any one or more of the following: i) your Username, ii) your Password, iii) Password Reset Questions, iv) your Security Device/ Digital Secure Key and/or v) your Security Code; you are liable for all claims, losses and consequences arising from or in connection with all transactions made using the services by or with the consent of that person.
c. If you have contributed to an unauthorised transaction, you may be liable for some or all of the loss resulting from the unauthorised transaction. Ways you can contribute to an unauthorized transaction include, but are not limited to, failing to take reasonable steps to observe any of your security duties referred to in these Terms and/or any unreasonable delay in notifying us of an actual or possible disclosure to any other person of your Username or Password or Password Reset Questions or Security Code and/or unauthorised use, control or loss of your Security Device.	c. If you have contributed to an unauthorised transaction, you may be liable for some or all of the loss resulting from the unauthorised transaction. Ways you can contribute to an unauthorized transaction include, but are not limited to, failing to take reasonable steps to observe any of your security duties referred to in these Terms and/or any unreasonable delay in notifying us of an actual or possible disclosure to any other person of your Username or Password or Password Reset Questions or Security Code and/or unauthorised use, control or loss of your Security Device/ Mobile device on which Digital Secure Key is used.
d. If you have reported the following as soon as reasonably practicable an actual or possible disclosure of your Username or	d. If you have reported the following as soon as reasonably practicable an actual or possible disclosure of your Username or

Password or Password Reset Questions or Security Code and/or unauthorised use, control or loss of your Security Device. to us, and HSBC has received this report, you will not be liable for the loss incurred after HSBC has received this report unless you have acted fraudulently or negligently.	Password or Password Reset Questions or Security Code and/or unauthorised use, control or loss of your Security Device/ Mobile device on which Digital Secure Key is used. to us, and HSBC has received this report, you will not be liable for the loss incurred after HSBC has received this report unless you have acted fraudulently or negligently.
11. SECURITY DEVICE/ DIGITAL SECURE KEY	**11. SECURITY DEVICE/ DIGITAL SECURE KEY**
We will make all reasonable efforts to ensure that the Security Device provided to you will perform as necessary to permit access to the services as and when required. You must notify us immediately if any Security Device fails to function correctly and the only obligations that we have in respect of such Security Device is to replace the same with a new Security Device for a fee which we shall determine the rate at our discretion from time to time, except under the following conditions: a. Upon the defective Security Device being returned to us within 90 days of its date of issue; and b. If we are satisfied that there is no default or negligence on your part which results in or contributes to the Security Device's failure to function correctly. Other than as specified in this Clause 11(a), we shall have no other liability in relation to this Security Device including, without limitation, liability for breach of any implied term as to satisfactory quality, merchantability or fitness for purpose of any Security Device. In addition, we cannot be held liable for any loss or damages incurred or suffered by you arising	a. We will make all reasonable efforts to ensure that the Security Device/ Digital Secure Key provided to you will perform as necessary to permit access to the services as and when required. b. You must notify us immediately if any Security Device fails to function correctly and the only obligations that we have in respect of such Security Device is to replace the same with a new Security Device for a fee which we shall determine the rate at our discretion from time to time, except under the following conditions: i) Upon the defective Security Device being returned to us within 90 days of its date of issue; and ii) If we are satisfied that there is no default or negligence on your part which results in or contributes to the Security Device's failure to function correctly. Other than as specified in this Clause 11(a), we shall have no other liability in relation to this Security Device including, without limitation, liability for breach of any implied term as to satisfactory quality, merchantability or fitness for purpose of any Security Device.

from your failure to safe-keep and/or use the Security Device in accordance with our instructions and recommendations.	In addition, we cannot be held liable for any loss or damages incurred or suffered by you arising from your failure to safe-keep and/or use the Security Device in accordance with our instructions and recommendations.
N/A	c. From February 2021, unless the Bank decides otherwise, Digital Secure Key feature shall be the default instrument (replacing Security Device) to generate Security Code for Personal Internet Banking. i) If you are currently using Security Device, as soon as you succesfully activate Digital Secure Key feature, your Security Device shall be deactivated immediately. ii) You can defer the Digital Secure Key activation within a certain period ("Deferment period") prescribed by us. During this Deferment period, you can still use your Security Device as well as the HSBC Vietnam app as usual. iii) After the Deferment period ends, if you have not successfully activated Digital Secure Key feature, you can still continue to use your Security Device to access and use services available on Personal Internet Banking. However, you cannot use the HSBC Vietnam app until you activate Digital Secure Key successfully. iv) In case you have activated Digital Secure Key successfully but then want to switch back to Security Device, provided that the Security Device is availably provided/accepted by

	the Bank, you shall have to follow our procedures applied at that time for changing Security code generating method as well as bear all the applicable fees and charges (if any). v) When any mobile device of yours on which the Digital Secure Key feature is used (deliberately or undeliberately)become malfunction, has its security compromised or cannot maintain security measures required or recommended by the Bank, or is no longer under your own control, including (but not limited) the following circumstances: broken, damaged, lost, stolen, replaced, hacked, jail-broken or rooted or data compromised, etc., you must immediatly remove that mentioned mobile device from the mobile device list registered for using HSBC Vietnam app via: (i) HSBC Vietnam app installed on another compatible mobile device (depending on the availablility of the relevant features on the HSBC Vietnam app from time to time); (ii) our Contact Center, or (iii) using any other methods provided by the Bank from time to time.
16. GENERAL	**16. GENERAL**
c. Indemnity: By your access, use and/or continued use of these services Website, you signify your agreement to indemnify and to keep indemnified HSBC, its directors, employees, nominees and agents fully against all actions, liabilities, costs, claims, losses, damages, proceedings and/or expenses (including all legal costs on	c. Indemnity: By your access, use and/or continued use of these services Website, you signify your agreement to indemnify and to keep indemnified HSBC, its directors, employees, nominees and agents fully against all actions, liabilities, costs, claims, losses, damages, proceedings and/or expenses (including all legal costs on

an indemnity basis) suffered or incurred by us including but not limited to, in connection with or arising from: ii) any unauthorised instructions (including but not limited to, instructions from unauthorised person(s) and/or instructions transmitted due to unauthorised use of the Username and/or Password, Password Reset Questions and/or Security Code and/or Security Device) that might be transmitted through Personal Internet Banking or any instructions which are incomplete, inaccurate or garbled; iv) any breach or non-observance of any of these Terms by you or by any other unauthorized person(s) using your Username, Password, Password Reset Questions and Security Device;	an indemnity basis) suffered or incurred by us including but not limited to, in connection with or arising from: ii) any unauthorised instructions (including but not limited to, instructions from unauthorised person(s) and/or instructions transmitted due to unauthorised use of the Username and/or Password, Password Reset Questions and/or Security Code and/or Security Device/ Digital Secure Key) that might be transmitted through Personal Internet Banking or any instructions which are incomplete, inaccurate or garbled; iv) any breach or non-observance of any of these Terms by you or by any other unauthorized person(s) using your Username, Password, Password Reset Questions and Security Device/ Digital Secure Key;
CURRENT PHONEBANKING SERVICES TERMS AND CONDITIONS	**PHONEBANKING SERVICES TERMS AND CONDITIONS**
3. OPERATION OF PHONEBANKING SERVICES The Customer may use PhoneBanking Services to: (a) enquire as to the balance of Account; (b) obtain information on recent transactions performed on Account; (c) transfer of funds from the Dedicated Transferor Account to the Credit Card Accounts of the Customer with which the PhoneBanking Services are established within the pre-defined dedicated transfer limits;	**3. OPERATION OF PHONEBANKING SERVICES** The Customer may use PhoneBanking Services to: (a) enquire as to the balance of Account; (b) obtain information on recent transactions performed on Account; (c) transfer of funds from the Dedicated Transferor Account to the Credit Card Accounts of the Customer with which the

(d) obtain information on exchange and deposit rates; (e) activate the Credit Card(s), including the activation via Contact Center, Interactive Voice Record or the SMS as designed by the Bank; (f) perform other types of banking and credit card services as the Bank may from time to time introduce.	PhoneBanking Services are established within the pre-defined dedicated transfer limits; (d) activate the Credit Card(s); (e) perform other types of banking and credit card services as the Bank may from time to time introduce.