|  |  |
| --- | --- |
| NGÂN HÀNG NHÀ NƯỚCVIỆT NAM | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc** |
| Số: /2024/TT-NHNN | *Hà Nội, ngày tháng năm 2024* |

**DỰ THẢO**

**Lần 1**

**THÔNG TƯ**

**Quy định về** **an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến  
trong ngành Ngân hàng**

*Căn cứ Luật Ngân hàng Nhà nước Việt Nam ngày 16 tháng 6 năm 2010;*

*Căn cứ Luật Các tổ chức tín dụng ngày 18 tháng 01 năm 2024;*

*Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;*

*Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;*

*Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;*

*Căn cứ Nghị định số 102/2022/NĐ-CP ngày 12 tháng12 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;*

*Theo đề nghị của Cục trưởng Cục Công nghệ thông tin,*

*Thống đốc Ngân hàng Nhà nước Việt Nam ban hành Thông tư quy định về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng.*

# Chương I

# QUY ĐỊNH CHUNG

## Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Thông tư này quy định các yêu cầu đảm bảo an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng, bao gồm:

a) Hoạt động ngân hàng (Nhận tiền gửi; Cấp tín dụng; Cung ứng dịch vụ thanh toán qua tài khoản);

b) Dịch vụ trung gian thanh toán;

c) Dịch vụ thông tin tín dụng;

d) Các hoạt động kinh doanh khác được Thống đốc Ngân hàng Nhà nước chấp thuận;

đ) Các hoạt động kinh doanh khác theo quy định của Thống đốc Ngân hàng Nhà nước.

2. Thông tư này áp dụng đối với các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, công ty thông tin tín dụng (sau đây gọi chung là đơn vị).

## Điều 2. Giải thích từ ngữ và thuật ngữ

Trong Thông tư này, các từ ngữ dưới đây được hiểu như sau:

1. *Dịch vụ trực tuyến trong ngành Ngân hàng* (gọi tắt là dịch vụ Online Banking) là dịch vụ quy định tại khoản 1 Điều 1 Thông tư này được các đơn vị cung cấp cho khách hàng trên môi trường mạng.
2. *Hệ thống Online Banking* là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu, hệ thống mạng truyền thông và an ninh bảo mật để sản xuất, truyền nhận, thu thập, xử lý, lưu trữ và trao đổi thông tin số phục vụ cho việc quản lý và cung cấp dịch vụ Online Banking.
3. *Phần mềm ứng dụng Online Banking* là phần mềm ứng dụng cung cấp dịch vụ Online Banking.
4. *Mobile Banking* là phần mềm ứng dụng Online Banking cài đặt trên thiết bị di động.
5. *Khách hàng* là các tổ chức, cá nhân sử dụng dịch vụ Online Banking.
6. *Mã khóa bí mật dùng một lần (One Time Password - OTP)* là mã khóa bí mật có giá trị sử dụng một lần và có hiệu lực trong một khoảng thời gian nhất định, thường được sử dụng như một yếu tố thứ 2 để xác thực người dùng truy cập ứng dụng hoặc thực hiện giao dịch Online Banking.
7. *Xác thực đa yếu tố*là phương pháp xác thực yêu cầu tối thiểu hai yếu tố để chứng minh tính đúng đắn của một danh tính. Xác thực đa yếu tố dựa trên những thông tin mà người dùng biết (số PIN, mã khóa bí mật,…) cùng với những gì mà người dùng có (thẻ thông minh, thiết bị token, thiết bị di động) hoặc những dấu hiệu sinh trắc học của người dùng để xác minh danh tính.
8. *Xác thực giao dịch điện tử* là hình thức xác nhận bằng phương tiện điện tử để thể hiện sự chấp thuận của khách hàng đối với giao dịch điện tử.
9. *Mã hóa điểm đầu đến điểm cuối (end to end encryption)* là cơ chế mã hóa an toàn thông tin ở điểm đầu trước khi gửi đi và chỉ được giải mã sau khi nhận được tại điểm cuối trong quá trình trao đổi thông tin giữa các ứng dụng, các thiết bị trong hệ thống nhằm hạn chế rủi ro bị lộ, lọt thông tin trên đường truyền.
10. *SMS OTP, Voice OTP, Email OTP* là các hình thức xác thực thông qua mã OTP gửi qua tin nhắn SMS, qua cuộc gọi thoại, qua thư điện tử.
11. *Thẻ ma trận OTP* là hình thức xác thực thông qua mã OTP được xác định từ một bảng 2 chiều (dòng, cột), tương ứng với mỗi dòng, cột là một mã OTP.
12. *Soft OTP* là hình thức xác thực thông qua mã OTP tạo bởi phần mềm cài đặt trên thiết bị di động của khách hàng. Soft OTP có 02 loại:
13. Soft OTP loại cơ bản: Mã OTP được sinh ngẫu nhiên theo thời gian, đồng bộ với hệ thống Online Banking.
14. Soft OTP loại nâng cao: Mã OTP được tạo kết hợp với mã của từng giao dịch. Khi thực hiện giao dịch, hệ thống Online Banking tạo ra một mã giao dịch thông báo cho khách hàng, khách hàng hoặc phần mềm tự động nhập mã giao dịch vào Soft OTP để Soft OTP tạo ra mã OTP.
15. *Token OTP* là hình thức xác thực thông qua mã OTP tạo bởi thiết bị chuyên dụng. Token OTP có 02 loại:
16. Token OTP loại cơ bản: Mã OTP được tạo một cách ngẫu nhiên theo thời gian, đồng bộ với hệ thống Online Banking.
17. Token OTP loại nâng cao: Mã OTP được tạo ra kết hợp với mã của từng giao dịch. Khi thực hiện giao dịch, hệ thống Online Banking tạo ra một mã giao dịch thông báo cho khách hàng, khách hàng nhập mã giao dịch vào Token OTP để thiết bị tạo ra mã OTP.
18. *Xác thực hai kênh* là hình thức xác thực khi khách hàng thực hiện giao dịch, hệ thống Online Banking sẽ gửi thông tin yêu cầu xác thực giao dịch đến thiết bị di động của khách hàng qua kênh thoại hoặc qua mã USSD hoặc qua phần mềm chuyên dụng; khách hàng phản hồi trực tiếp qua kênh đã kết nối để xác nhận hoặc không xác nhận thực hiện giao dịch.
19. *Dấu hiệu nhận dạng sinh trắc học* là những thuộc tính vật lý, đặc điểm sinh học cá biệt và ổn định của một người để nhận diện, phân biệt người này với người khác như khuôn mặt, vân tay, mống mắt, ADN, giọng nói.
20. *FIDO* là tiêu chuẩn xác thực do Liên minh Xác thực trực tuyến thế giới FIDO Alliance ban hành.
21. *Chữ ký điện tử an toàn* là chữ ký điện tử bao gồm Chữ ký điện tử chuyên dùng bảo đảm an toàn hoặc chữ ký số hoặc chữ ký điện tử nước ngoài được công nhận theo quy định của pháp luật.
22. *CCCD* là thẻ Căn cước công dân hoặc thẻ Căn cước do cơ quan Công an cấp.

## Điều 3. Nguyên tắc chung về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin cho việc cung cấp dịch vụ Online Banking

1. Hệ thống Online Banking phải tuân thủ theo quy định về bảo đảm an toàn hệ thống thông tin cấp độ 3 trở lên theo quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và quy định của Ngân hàng Nhà nước về an toàn hệ thống thông tin trong hoạt động ngân hàng.

2. Đảm bảo tính bí mật, tính toàn vẹn của thông tin khách hàng; đảm bảo tính sẵn sàng của hệ thống Online Banking để cung cấp dịch vụ một cách liên tục.

3. Các giao dịch của khách hàng được đánh giá mức độ rủi ro tối thiểu theo từng nhóm khách hàng, loại giao dịch, hạn mức giao dịch (nếu có) và trên cơ sở đó cung cấp hình thức xác thực giao dịch phù hợp cho khách hàng lựa chọn, tuân thủ các quy định sau:

a) Áp dụng xác thực đa yếu tố khi thay đổi thông tin định danh khách hàng;

b) Áp dụng các hình thức xác thực cho từng nhóm khách hàng, loại giao dịch, hạn mức giao dịch theo quy định tại Thông tư này;

c) Đối với giao dịch gồm nhiều bước, phải áp dụng tối thiểu biện pháp xác thực tại bước phê duyệt cuối cùng.

4. Thực hiện kiểm tra, đánh giá an ninh, bảo mật hệ thống Online Banking theo định kỳ hàng năm.

5. Thường xuyên nhận dạng rủi ro, nguy cơ gây ra rủi ro và xác định nguyên nhân gây ra rủi ro, kịp thời có biện pháp phòng ngừa, kiểm soát và xử lý rủi ro trong cung cấp dịch vụ ngân hàng trên Internet.

6. Các trang thiết bị hạ tầng kỹ thuật công nghệ thông tin cung cấp dịch vụ Online Banking phải có bản quyền, nguồn gốc, xuất xứ rõ ràng. Với các trang thiết bị sắp hết vòng đời sản phẩm và sẽ không được nhà sản xuất tiếp tục hỗ trợ, đơn vị phải có kế hoạch nâng cấp, thay thế theo thông báo của nhà sản xuất, bảo đảm các trang thiết bị hạ tầng có khả năng cài đặt phiên bản phần mềm mới.

# Chương II

# CÁC QUY ĐỊNH CỤ THỂ

# Mục 1. HẠ TẦNG KỸ THUẬT CỦA HỆ THỐNG ONLINE BANKING

## Điều 4. Hệ thống mạng, truyền thông và an ninh bảo mật

Đơn vị phải thiết lập hệ thống mạng, truyền thông và an ninh bảo mật đạt yêu cầu tối thiểu sau:

1. Có các giải pháp an ninh bảo mật tối thiểu gồm:

a) Tường lửa ứng dụng;

b) Tường lửa cơ sở dữ liệu;

c) Hệ thống giám sát, cảnh báo tập trung đối với các hành vi tấn công hoặc hành vi bất thường.

2. Thông tin khách hàng không được lưu trữ tại phân vùng kết nối Internet và phân vùng DMZ (phân vùng trung gian giữa mạng nội bộ và mạng Internet).

3. Thiết lập chính sách hạn chế tối đa các dịch vụ, cổng kết nối vào hệ thống Online Banking.

4. Kết nối từ bên ngoài mạng nội bộ vào hệ thống Online Banking để quản trị chỉ được thực hiện trong trường hợp không thể kết nối từ mạng nội bộ và bảo đảm an toàn, tuân thủ tối thiểu các quy định sau:

a) Phải được người có thẩm quyền phê duyệt sau khi xem xét mục đích, cách thức kết nối;

b) Phải có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn như sử dụng mạng riêng ảo hoặc phương án tương đương;

c) Thiết bị kết nối phải được cài đặt các phần mềm bảo đảm an ninh bảo mật;

d) Phải sử dụng biện pháp xác thực đa yếu tố khi đăng nhập hệ thống;

đ) Sử dụng giao thức truyền thông được mã hóa an toàn và không lưu mã khóa bí mật tại các phần mềm tiện ích.

5. Đường truyền kết nối mạng cung cấp dịch vụ phải bảo đảm tính sẵn sàng cao và khả năng cung cấp dịch vụ liên tục.

## Điều 5. Hệ thống máy chủ và phần mềm hệ thống

1. Yêu cầu đối với máy chủ

a) Hiệu năng sử dụng trung bình hàng tháng tối đa 80% công suất thiết kế;

b) Hệ thống Online Banking phải có máy chủ dự phòng tại chỗ bảo đảm tính sẵn sàng cao;

c) Tách biệt về lô-gíc hoặc vật lý với các máy chủ hoạt động nghiệp vụ khác;

d) Phải được kiểm tra, gia cố an toàn, bảo mật (hardening) cho hệ điều hành, cập nhật các bản vá lỗi thường xuyên.

2. Đơn vị phải lập danh mục các phần mềm được phép cài đặt trên máy chủ. Định kỳ tối thiểu sáu tháng một lần cập nhật, kiểm tra, đảm bảo tuân thủ danh mục này.

## Điều 6. Hệ quản trị cơ sở dữ liệu

1. Hệ quản trị cơ sở dữ liệu phải có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu.

2. Hệ thống Online Banking phải có cơ sở dữ liệu dự phòng thảm họa có khả năng thay thế cơ sở dữ liệu chính và bảo đảm đầy đủ, toàn vẹn dữ liệu giao dịch trực tuyến của khách hàng.

3. Đơn vị phải có biện pháp giám sát, ghi nhật ký truy cập cơ sở dữ liệu và các thao tác khi truy cập cơ sở dữ liệu.

## Điều 7. Phần mềm ứng dụng Online Banking

1. Các yêu cầu về an toàn, bảo mật phải được xác định trước khi phát triển phần mềm và tổ chức, triển khai trong quá trình phát triển (phân tích, thiết kế, xây dựng, kiểm thử), vận hành chính thức và duy trì hoạt động phần mềm. Các hồ sơ, tài liệu về an toàn, bảo mật của phần mềm phải được hệ thống hóa, lưu trữ, cập nhật đồng bộ khi hệ thống chính thức có thay đổi và kiểm soát chặt chẽ, hạn chế tiếp cận.

2. Đơn vị phải kiểm soát mã nguồn phần mềm với các yêu cầu tối thiểu:

a) Định kỳ hoặc khi có thay đổi phần mềm ứng dụng, đơn vị phải kiểm tra mã nguồn nhằm loại trừ các đoạn mã độc hại, các lỗ hổng bảo mật. Nhân sự thực hiện kiểm tra phải độc lập với nhân sự phát triển mã nguồn ứng dụng;

b) Chỉ định cụ thể các cá nhân chịu trách nhiệm quản lý mã nguồn của phần mềm ứng dụng;

c) Mã nguồn phải được lưu trữ an toàn tại ít nhất hai địa điểm tách biệt về địa lý và có biện pháp bảo vệ tính toàn vẹn của mã;

d) Trường hợp mã nguồn phần mềm do bên thứ ba phát triển, cung cấp, đơn vị phải yêu cầu bên cung cấp ký cam kết mã nguồn phần mềm là hợp pháp, không giả mạo; cam kết thực hiện các thoả thuận về việc chỉnh sửa mã nguồn khi bảo hành, bảo trì phần mềm.

đ) Trước khi cung cấp, bàn giao mã nguồn phần mềm, đơn vị yêu cầu bên cung cấp phải kiểm tra, xử lý, khắc phục các lỗ hổng bảo mật trong mã nguồn. Trường hợp không được bàn giao mã nguồn, khi ký hợp đồng hoặc nghiệm thu hợp đồng, đơn vị phải yêu cầu bên cung cấp ký cam kết: không có các đoạn mã độc hại trong phần mềm ứng dụng mua ngoài.

3. Phần mềm ứng dụng Online Banking phải được kiểm tra, thử nghiệm trước khi vận chính thức đáp ứng các yêu cầu tối thiểu sau:

a) Lập và phê duyệt kế hoạch, kịch bản thử nghiệm phần mềm ứng dụng Online Banking, trong đó nêu rõ các điều kiện về tính an toàn, bảo mật phải được đáp ứng;

b) Phát hiện và loại trừ các lỗi, các gian lận có thể xảy ra khi nhập số liệu đầu vào;

c) Đánh giá, dò quét phát hiện lỗ hổng, điểm yếu về mặt kỹ thuật. Đánh giá khả năng phòng chống các kiểu tấn công bao gồm nhưng không giới hạn: Injection (SQL, Xpath, LDAP…), Cross-site Scripting (XSS), Cross-site Request Forgery (XSRF), Server-Side Request Forgery(SSRS), Brute-Force và các loại lỗi bảo mật như: lỗi kiểm soát truy cập; lỗi nhận dạng và xác thực; lỗi mã hóa; lỗi thiết kế, cấu hình không an toàn; lỗi ghi nhật ký và giám sát bảo mật;

d) Ghi lại các lỗi và quá trình xử lý lỗi, đặc biệt là các lỗi về an toàn, bảo mật trong các báo cáo về kiểm tra thử nghiệm;

đ) Kiểm tra thử nghiệm các tính năng an toàn, bảo mật phải được thực hiện trên các trình duyệt (ứng dụng web) và phiên bản phần mềm hệ thống của thiết bị di động (ứng dụng mobile); có cơ chế kiểm tra, thông báo cho người dùng chạy ứng dụng trên các trình duyệt, phiên bản phần mềm hệ thống đã được kiểm tra và thử nghiệm an toàn.

4. Trước khi triển khai phần mềm ứng dụng mới, đơn vị phải đánh giá những rủi ro của quá trình triển khai đối với hoạt động nghiệp vụ, các hệ thống công nghệ thông tin liên quan và lập, triển khai các phương án hạn chế, khắc phục rủi ro.

5. Đơn vị thực hiện quản lý thay đổi phiên bản phần mềm ứng dụng đáp ứng các yêu cầu sau:

a) Xây dựng tài liệu phân tích đánh giá tác động của việc thay đổi đối với hệ thống hiện tại và các hệ thống có liên quan khác của đơn vị và được người có thẩm quyền phê duyệt trước khi thực hiện;

b) Các phiên bản phần mềm bao gồm cả mã nguồn cần được quản lý tập trung, lưu trữ, bảo mật và có cơ chế phân quyền cho từng thành viên, ghi nhật ký trong việc thao tác với các tập tin;

c) Thông tin về các phiên bản (thời gian cập nhật, người cập nhật, hướng dẫn cập nhật và các thông tin liên quan khác của phiên bản) phải được lưu lại;

d) Việc nâng cấp phiên bản phải căn cứ trên kết quả thử nghiệm và được người có thẩm quyền phê duyệt;

6. Các tính năng bắt buộc của phần mềm ứng dụng Online Banking:

a) Toàn bộ dữ liệu khi truyền trên môi trường mạng Internet được áp dụng cơ chế mã hóa điểm đầu đến điểm cuối;

b) Bảo đảm tính toàn vẹn của dữ liệu giao dịch, mọi sửa đổi bất hợp pháp phải được phát hiện trong quá trình xử lý giao dịch, lưu trữ dữ liệu;

c) Kiểm soát phiên giao dịch: hệ thống có cơ chế tự động ngắt phiên giao dịch khi người sử dụng không thao tác trong một khoảng thời gian do đơn vị quy định hoặc áp dụng các biện pháp bảo vệ khác;

d) Có chức năng che giấu đối với việc hiển thị các mã khóa bí mật dùng để đăng nhập vào hệ thống;

đ) Có các chức năng:

(i) Chống đăng nhập tự động khi khách hàng truy cập bằng trình duyệt;

(ii) Yêu cầu thay đổi mã khóa bí mật khi đăng nhập trong trường hợp khách hàng được cấp phát mã khóa bí mật mặc định lần đầu;

(iii) Thông báo cho khách hàng khi mã khóa bí mật sắp hết hiệu lực sử dụng. Cho phép khách hàng lựa chọn thay đổi hoặc tiếp tục sử dụng mã khóa bí mật cũ. Trường hợp tiếp tục sử dụng mã khóa bí mật cũ, phải yêu cầu khách hàng xác thực lại mã khóa bí mật cũ này;

(iv) Hủy hiệu lực của mã khóa bí mật khi hết hạn sử dụng;

(v) Khóa tài khoản truy cập trong trường hợp bị nhập sai mã khóa bí mật liên tiếp quá số lần do đơn vị quy định (nhưng không quá 10 lần), đơn vị chỉ mở khóa tài khoản khi khách hàng yêu cầu và phải xác thực khách hàng trước khi thực hiện mở khóa tài khoản, bảo đảm chống gian lận, giả mạo;

e) Đối với khách hàng là tổ chức, phần mềm ứng dụng được thiết kế để bảo đảm việc thực hiện giao dịch bao gồm tối thiểu hai bước: tạo, phê duyệt giao dịch. Trong trường hợp khách hàng là tổ chức được pháp luật cho phép áp dụng chế độ kế toán đơn giản, việc thực hiện giao dịch tương tự như khách hàng cá nhân;

g) Trong trường hợp không sử dụng xác thực đa yếu tố khi đăng nhập, phải có chức năng thông báo việc đăng nhập lần đầu phần mềm ứng dụng Online Banking hoặc việc đăng nhập phần mềm ứng dụng Online Banking trên thiết bị khác với thiết bị thực hiện đăng nhập phần mềm ứng dụng Online Banking lần gần nhất qua SMS hoặc các kênh khác do khách hàng đăng ký (điện thoại, thư điện tử…);

7. Phần mềm ứng dụng Online Banking phải có chức năng lưu trữ thông tin về thiết bị thực hiện các giao dịch trực tuyến của khách hàng và nhật ký (log) xác thực giao dịch tối thiểu trong vòng 03 tháng, trong đó gồm:

a) Thông tin định danh về thiết bị:

(i) Đối với thiết bị di động: thông tin định danh duy nhất của thiết bị (ví dụ như: số IMEI hoặc Serial hoặc WLAN MAC hoặc Android ID hoặc thông tin định danh khác);

(ii) Đối với máy tính: thông tin định danh duy nhất của máy tính (ví dụ như địa chỉ MAC hoặc thông tin định danh thiết bị khác);

b) Nhật ký (log) xác thực giao dịch tối thiểu gồm: biện pháp xác thực, thời gian xác thực, mã giao dịch được xác thực, mã khách hàng.

## Điều 8. Phần mềm ứng dụng Mobile Banking

Phần mềm ứng dụng Mobile Banking do đơn vị cung cấp phải đảm bảo tuân thủ các quy định tại Điều 7 Thông tư này và các yêu cầu sau:

1. Phải được đăng ký và quản lý tại kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động và chỉ rõ đường dẫn trên trang điện tử hoặc cổng thông tin điện tử để khách hàng tải và cài đặt phần mềm ứng dụng Mobile Banking.

2. Phải được áp dụng các biện pháp bảo vệ để hạn chế dịch ngược.

3. Phải xác thực người dùng khi truy cập và không có tính năng ghi nhớ mã khóa bí mật truy cập.

4. Đối với khách hàng cá nhân, phần mềm ứng dụng Mobile Banking phải xác thực khách hàng trước khi cho phép khách hàng thực hiện giao dịch lần đầu hoặc trước khi khách hàng thực hiện giao dịch trên thiết bị khác với thiết bị thực hiện giao dịch tại ứng dụng Mobile Banking lần gần nhất:

a) Bằng dấu hiệu nhận dạng sinh trắc học của khách hàng: (i) khớp đúng với dữ liệu sinh trắc học được lưu trong chip CCCD của khách hàng do cơ quan Công an cấp; (ii) hoặc khớp đúng thông qua xác thực tài khoản định danh điện tử của khách hàng trong do hệ thống định danh và xác thực điện tử tạo lập; (iii) hoặc khớp đúng thông qua gặp mặt trực tiếp với khách hàng cá nhân là người nước ngoài hoặc khách hàng cá nhân không phải làm CCCD gắn chíp theo quy định của pháp luật.

b) Hoặc bằng dấu hiệu nhận dạng sinh trắc học của khách hàng khớp đúng với dữ liệu sinh trắc học được lưu trong cơ sở dữ liệu sinh trắc học về khách hàng đã thu thập và kiểm tra (kiểm tra theo các biện pháp tại điểm a khoản 4 Điều này hoặc kiểm tra khớp đúng với dấu hiệu sinh trắc học trong cơ sở dữ liệu quốc gia về dân cư), kết hợp với hình thức xác thực SMS OTP hoặc Voice OTP hoặc Soft OTP hoặc Token OTP.

# Mục 2. XÁC THỰC GIAO DỊCH ONLINE BANKING

## Điều 9. Xác thực khách hàng truy cập dịch vụ Online Banking

1. Khách hàng đăng ký sử dụng dịch vụ Online Banking phải được đơn vị cấp tài khoản định danh. Tài khoản định danh gồm tên đăng nhập và tối thiểu một hình thức xác thực quy định tại Điều 11 Thông tư này, đáp ứng các yêu cầu sau:

a) Tên đăng nhập phải có độ dài tối thiểu sáu ký tự; không được sử dụng toàn bộ ký tự trùng nhau hoặc liên tục theo thứ tự trong bảng chữ cái, chữ số;

b) Trường hợp sử dụng hình thức xác thực là mã PIN hoặc mã khóa bí mật khi truy cập dịch vụ Online Banking: mã PIN, mã khóa bí mật phải có độ dài tối thiểu tám ký tự, cấu tạo gồm các ký tự: số, chữ hoa, chữ thường và các ký tự đặc biệt. Thời gian hiệu lực của mã PIN, mã khóa bí mật tối đa 12 tháng.

2. Khách hàng sử dụng tài khoản định danh đã được đơn vị cấp để truy cập sử dụng dịch vụ Online Banking.

## Điều 10. Xác thực giao dịch điện tử

1. Đối với giao dịch thanh toán trực tuyến (ngoại trừ thanh toán thẻ quốc tế): đơn vị thực hiện phân loại giao dịch theo các nhóm loại hình giao dịch tại Phụ lục 01 ban hành kèm theo Thông tư này và áp dụng các hình thức xác thực giao dịch điện tử theo quy định tại Điều 11 và Phụ lục 02 ban hành kèm theo Thông tư này.

2. Đối với các giao dịch ngân hàng trực tuyến khác: đơn vị áp dụng tối thiểu một trong các hình thức xác thực giao dịch điện tử theo quy định tại Điều 11 Thông tư này trên cơ sở đánh giá rủi ro tối thiểu theo từng nhóm khách hàng, loại giao dịch, hạn mức giao dịch (nếu có) và tuân thủ quy định pháp luật về giao dịch điện tử.

## Điều 11. Các hình thức xác thực giao dịch điện tử

1. Hình thức xác thực bằng mã PIN hoặc mã khóa bí mật phải đáp ứng yêu cầu:

a) Độ dài tối thiểu 4 ký tự;

b) Yêu cầu thay đổi mã PIN hoặc mã khóa bí mật trong trường hợp khách hàng được cấp phát mã PIN hoặc mã khóa bí mật mặc định lần đầu;

c) Vô hiệu hóa mã PIN hoặc mã khóa bí mật trong trường hợp bị nhập sai liên tiếp quá số lần do đơn vị quy định (nhưng không quá 10 lần). Đơn vị chỉ mở lại khi khách hàng yêu cầu và phải xác thực khách hàng trước khi thực hiện, bảo đảm chống gian lận, giả mạo.

2. Hình thức xác thực bằng SMS OTP, Voice OTP, Email OTP phải đáp ứng yêu cầu:

a) OTP gửi tới khách hàng phải kèm thông tin cảnh báo để khách hàng nhận biết được mục đích của OTP;

b) OTP có hiệu lực tối đa không quá 03 phút.

3. Hình thức xác thực bằng thẻ ma trận OTP phải đáp ứng yêu cầu:

a) Thẻ ma trận OTP có thời hạn sử dụng tối đa 01 năm kể từ ngày đăng ký thẻ;

b) OTP có hiệu lực tối đa không quá 02 phút.

4. Hình thức xác thực bằng Soft OTP phải đáp ứng yêu cầu:

a) Soft OTP phải được đăng ký, quản lý tại kho ứng dụng chính thức của hãng cung cấp hệ điều hành cho thiết bị di động và chỉ rõ đường dẫn trên trang điện tử hoặc cổng thông tin điện tử để khách hàng tải và cài đặt phần mềm;

b) Soft OTP phải yêu cầu kích hoạt trước khi sử dụng. Mã kích hoạt sử dụng Soft OTP do đơn vị cung cấp cho khách hàng và chỉ được sử dụng để kích hoạt trên một thiết bị di động. Mã kích hoạt phải được thiết lập thời hạn hiệu lực sử dụng;

c) Soft OTP phải có tính năng kiểm soát truy cập. Trường hợp khách hàng xác thực truy cập sai liên tiếp quá số lần do đơn vị quy định (nhưng không quá 10 lần), Soft OTP phải tự động khóa không cho khách hàng sử dụng tiếp;

d) OTP có hiệu lực tối đa không quá 02 phút.

5. Hình thức xác thực bằng OTP token phải đáp ứng yêu cầu: OTP có hiệu lực tối đa không quá 02 phút.

6. Hình thức xác thực hai kênh phải đáp ứng yêu cầu: yêu cầu xác thực có hiệu lực tối đa không quá 02 phút.

7. Hình thức xác thực FIDO phải đáp ứng yêu cầu: được Liên minh Xác thực trực tuyến thế giới (FIDO Alliance) cấp chứng chỉ.

8. Hình thức xác thực bằng chữ ký điện tử phải đáp ứng yêu cầu: chữ ký điện tử phải đáp ứng quy định của pháp luật về chữ ký điện tử.

9. Hình thức xác thực bằng dấu hiệu nhận dạng sinh trắc học phải đáp ứng yêu cầu:

a) Trường hợp xác thực bằng dấu hiệu nhận dạng sinh trắc học gắn liền với thiết bị di động: chỉ cho phép kích hoạt sử dụng sau khi có sự đồng ý của khách hàng và khách hàng đã thực hiện một số lần (do đơn vị quy định) giao dịch thành công bằng hình thức xác thực khác.

b) Trường hợp xác thực bằng dấu hiệu nhận dạng sinh trắc học thông qua CCCD gắn chíp của khách hàng do cơ quan Công an cấp; hoặc thông qua xác thực tài khoản định danh điện tử của khách hàng do hệ thống định danh và xác thực điện tử tạo lập; hoặc thông qua cơ sở dữ liệu sinh trắc học về khách hàng đã thu thập và kiểm tra (kiểm tra theo các biện pháp tại điểm a khoản 4 Điều 8 Thông tư này hoặc kiểm tra khớp đúng với dấu hiệu sinh trắc học trong cơ sở dữ liệu quốc gia về dân cư) phải tuân thủ tối thiểu các quy định sau:

(i) Đơn vị lựa chọn công nghệ xác thực sinh trắc học có độ chính xác được xác định theo tiêu chuẩn quốc tế như sau (hoặc tương đương):

- Có tỷ lệ chấp nhận sai (FAR) < 0.01% theo tiêu chuẩn FIDO Biometric Requirement.

- Có tỷ lệ từ chối sai (FRR) < 5% theo tiêu chuẩn FIDO Biometric Requirement.

(ii) Có khả năng phát hiện phát hiện các cuộc tấn công giả mạo dấu hiệu sinh trắc học của vật thể sống (Presentation Attack Detection - PAD) dựa trên các tiêu chuẩn quốc tế (như NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management hoặc ISO 30107 - Biometric presentation attack detection hoặc FIDO Biometric Requirements) để phòng chống gian lận, giả mạo khách hàng qua hình ảnh, video, mặt nạ 3D.

c) Vô hiệu hóa hình thức xác thực bằng sinh trắc học trong trường hợp xác thực sai liên tiếp quá số lần do đơn vị quy định (nhưng không quá 10 lần). Đơn vị chỉ mở lại khi khách hàng yêu cầu và phải xác thực khách hàng trước khi thực hiện, bảo đảm chống gian lận, giả mạo.

# Mục 3. QUẢN LÝ VẬN HÀNH

## Điều 12. Quản lý nhân sự quản trị, vận hành hệ thống Online Banking

1. Đơn vị phải phân công nhân sự giám sát, theo dõi hoạt động của hệ thống, phát hiện và xử lý các sự cố kỹ thuật, các cuộc tấn công mạng.

2. Đơn vị phải phân công nhân sự tiếp nhận thông tin, hỗ trợ khách hàng, kịp thời liên lạc với khách hàng khi phát hiện các giao dịch bất thường.

3. Nhân sự quản trị, giám sát và vận hành hệ thống Online Banking phải tham gia các khóa đào tạo cập nhật kiến thức an ninh, bảo mật hằng năm.

4. Việc cấp phát, phân quyền tài khoản quản trị hệ thống Online Banking phải được theo dõi, giám sát bởi bộ phận độc lập với bộ phận cấp phát tài khoản.

## Điều 13. Quản lý hoạt động của môi trường vận hành hệ thống Online Banking

1. Đơn vị không cài đặt, lưu trữ phần mềm phát triển ứng dụng, mã nguồn trên môi trường vận hành.

2. Hoạt động quản trị, giám sát và vận hành phải đáp ứng các yêu cầu sau:

a) Máy tính của nhân sự quản trị, giám sát và vận hành phải được cài đặt phần mềm phòng chống mã độc;

b) Việc kết nối quản trị, giám sát và vận hành hệ thống phải qua các máy chủ trung gian hoặc các hệ thống quản trị tập trung an toàn, có kiểm soát, không thực hiện trực tiếp từ máy tính của người dùng;

c) Việc sử dụng tài khoản có quyền quản trị, giám sát và vận hành phải được giới hạn trong khoảng thời gian đủ để thực hiện công việc và phải được thu hồi trong vòng 15 phút kể từ khi kết thúc công việc;

d) Phải có biện pháp giám sát việc sử dụng tài khoản có quyền quản trị, giám sát và vận hành, có cảnh báo khi có tác động bất thường vào cơ sở dữ liệu, ứng dụng.

3. Đơn vị phải thiết lập chính sách đối với các máy tính thực hiện quản trị, giám sát và vận hành hệ thống Online Banking chỉ được phép kết nối đến hệ thống Online Banking hoặc các hệ thống thông tin khác của đơn vị để phục vụ quản trị, giám sát và vận hành.

## Điều 14. Quản lý lỗ hổng, điểm yếu về mặt kỹ thuật

Đơn vị phải thực hiện quản lý các lỗ hổng, điểm yếu của hệ thống Online Banking với các nội dung cơ bản sau:

1. Có biện pháp phòng, chống, dò tìm phát hiện các thay đổi của trang tin điện tử, phần mềm ứng dụng Online Banking.

2. Thiết lập cơ chế phát hiện, phòng chống xâm nhập, tấn công mạng vào hệ thống Online Banking.

3. Phối hợp với các đơn vị quản lý nhà nước, các đối tác công nghệ thông tin kịp thời nắm bắt các sự cố tình huống mất an toàn, bảo mật thông tin để có biện pháp ngăn chặn kịp thời.

4. Cập nhật thông tin các lỗ hổng bảo mật được công bố có liên quan đến phần mềm hệ thống, hệ quản trị cơ sở dữ liệu và phần mềm ứng dụng theo thông tin từ Hệ thống tính điểm lỗ hổng phổ biến (Common Vulnerability Scoring System version 3 - CVSS v3 hoặc tương đương).

5. Thực hiện dò quét lỗ hổng, điểm yếu của hệ thống Online Banking tối thiếu mỗi năm một lần hoặc khi tiếp nhận được những thông tin liên quan đến lỗ hổng, điểm yếu mới. Đánh giá mức độ tác động, rủi ro của từng lỗ hổng, điểm yếu về mặt kỹ thuật được phát hiện của hệ thống và đưa ra phương án, kế hoạch xử lý.

6. Thực hiện triển khai cập nhật các bản vá bảo mật hoặc các biện pháp phòng ngừa kịp thời căn cứ theo đánh giá mức độ tác động, rủi ro:

a) Trong vòng 1 tháng sau khi công bố với lỗ hổng bảo mật được đánh giá ở mức nghiêm trọng;

b) Trong vòng 2 tháng sau khi công bố với lỗ hổng bảo mật được đánh giá ở mức cao;

c) Khoảng thời gian do đơn vị tự quyết định với lỗ hổng bảo mật được đánh giá ở mức trung bình hoặc thấp.

## Điều 15. Hệ thống quản trị, giám sát hoạt động của hệ thống Online Banking

1. Đơn vị phải thiết lập hệ thống giám sát, theo dõi hoạt động của hệ thống Online Banking. Hệ thống giám sát, theo dõi hoạt động của hệ thống Online Banking phải thu thập đầy đủ nhật ký (log) của các thành phần thuộc hệ thống Online Banking để phát hiện, điều tra các sự kiện bất thường hoặc các hành vi tấn công mạng.

2. Đơn vị phải xây dựng các tiêu chí và phần mềm để xác định các giao dịch bất thường dựa vào thời gian, vị trí địa lý, tần suất giao dịch, số tiền giao dịch, số lần đăng nhập sai quá quy định và các dấu hiệu bất thường khác.

## Điều 16. Đảm bảo hoạt động liên tục

Đơn vị phải xây dựng hệ thống dự phòng thảm hoạ, quy trình, kịch bản đảm bảo hoạt động liên tục cho hệ thống Online Banking theo quy định của Ngân hàng Nhà nước về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng. Ngoài ra, đơn vị phải thực hiện:

1. Phân tích, xác định các tình huống có thể gây mất an ninh thông tin và gián đoạn hoạt động của hệ thống Online Banking. Xác định, đánh giá mức độ rủi ro, khả năng có thể xảy ra đối với từng tình huống tối thiểu sáu tháng một lần. Lập danh sách các tình huống có mức độ rủi ro, khả năng có thể xảy ra theo các cấp độ cao, trung bình, chấp nhận được và thấp.

2. Xây dựng phương án (quy trình, kịch bản) xử lý khắc phục các tình huống có mức độ rủi ro, khả năng có thể xảy ra ở cấp độ cao và trung bình theo Khoản 1 Điều này. Xác định thời gian dừng hoạt động tối đa để phục hồi hệ thống, phục hồi dữ liệu cho phương án xử lý đối với từng tình huống. Tổ chức phổ biến phương án xử lý đến các nhân sự có liên quan để hiểu rõ nhiệm vụ, công việc cần phải thực hiện khi xử lý.

3. Bố trí nguồn nhân lực, tài chính và các phương tiện kỹ thuật để tổ chức diễn tập phương án xử lý với các tình huống có mức độ rủi ro, khả năng xảy ra cao theo định kỳ tối thiểu sáu tháng một lần.

4. Lập kế hoạch và tiến hành diễn tập các biện pháp đảm bảo hoạt động kinh doanh liên tục, lưu giữ các hồ sơ có liên quan và tổ chức đánh giá kết quả diễn tập.

# Mục 4. BẢO VỆ QUYỀN LỢI CỦA KHÁCH HÀNG

## Điều 17. Thông tin về dịch vụ Online Banking

1. Đơn vị phải công bố thông tin về dịch vụ Online Banking; bảo đảm khách hàng có khả năng tiếp cận được thông tin trước hoặc ngay tại thời điểm đăng ký sử dụng dịch vụ; thông tin công bố tối thiểu gồm có:

a) Cách thức cung cấp dịch vụ; cách thức truy cập dịch vụ Online Banking ứng với từng phương tiện truy cập;

b) Hạn mức giao dịch và các hình thức xác thực giao dịch tương ứng với từng hạn mức (nếu có);

c) Các trang thiết bị cần thiết để sử dụng dịch vụ; điều kiện với các trang bị được sử dụng;

d) Các rủi ro liên quan đến việc sử dụng dịch vụ Online Banking;

đ) Đối tác được đơn vị hợp tác để cung cấp dịch vụ Online Banking; phạm vi hợp tác liên quan đến việc chia sẻ, xử lý dữ liệu cá nhân của khách hàng (nếu có).

2. Đơn vị phải thông tin cho khách hàng về các điều khoản trong hợp đồng cung cấp, sử dụng dịch vụ Online Banking, tối thiểu gồm:

a) Quyền lợi và nghĩa vụ của khách hàng sử dụng dịch vụ Online Banking;

b) Trách nhiệm của đơn vị trong bảo mật dữ liệu cá nhân của khách hàng; cam kết không bán, tiết lộ dữ liệu cá nhân của khách hàng;

c) Các loại dữ liệu cá nhân của khách hàng mà đơn vị thu thập; cách thức đơn vị thu thập, sử dụng dữ liệu cá nhân của khách hàng;

d) Cam kết không chối bỏ, thay đổi trách nhiệm của đơn vị trong việc bảo đảm quyền lợi của khách hàng khi phát sinh sự cố mất an toàn dịch vụ ngân hàng điện tử liên quan đến đối tác của đơn vị tại điểm đ khoản 1 Điều này;

đ) Cam kết khả năng đảm bảo hoạt động liên tục của hệ thống Online Banking, tối thiểu gồm: thời gian gián đoạn cung cấp dịch vụ trong một lần, tổng thời gian gián đoạn cung cấp dịch vụ trong một năm;

e) Các nội dung khác của đơn vị đối với dịch vụ Online Banking (nếu có).

## Điều 18. Bảo đảm an toàn cho khách hàng trong giao dịch thanh toán thẻ trực tuyến

Các đơn vị cung cấp dịch vụ thanh toán thẻ trực tuyến phải triển khai các giải pháp giảm thiểu rủi ro cho khách hàng đăng ký sử dụng như sau:

1. Thông báo giao dịch thanh toán thẻ trực tuyến qua tin nhắn SMS hoặc thư điện tử hoặc phần mềm ứng dụng Mobile Banking hoặc các kênh liên lạc khác do khách hàng đăng ký.

2. Thiết lập tính năng cho phép hoặc không cho phép thanh toán trực tuyến.

3. Thiết lập hạn mức thanh toán thẻ trực tuyến trong ngày.

4. Thiết lập tính năng cho phép hoặc không cho phép thanh toán ở nước ngoài.

5. Triển khai giải pháp xác thực 3D Secure (hoặc tương đương) cho việc thanh toán trực tuyến với thẻ quốc tế.

## Điều 19. Hướng dẫn khách hàng sử dụng dịch vụ Online Banking

1. Đơn vị phải xây dựng quy trình, tài liệu hướng dẫn cài đặt, sử dụng các phần mềm, ứng dụng, thiết bị thực hiện các giao dịch Online Banking và cung cấp, hướng dẫn khách hàng sử dụng các quy trình, tài liệu này.

2. Đơn vị phải hướng dẫn khách hàng thực hiện các biện pháp đảm bảo an toàn, bảo mật khi sử dụng dịch vụ Online Banking, tối thiểu gồm các nội dung sau:

a) Bảo vệ bí mật mã khóa bí mật, mã PIN, OTP và không chia sẻ các thiết bị lưu trữ các thông tin này;

b) Cách thiết lập mã khóa bí mật, mã PIN và thay đổi mã khóa bí mật, mã PIN của tài khoản định danh;

c) Không dùng máy tính công cộng để truy cập, thực hiện giao dịch Online Banking; không nên sử dụng mạng WIFI công cộng khi sử dụng dịch vụ Online Banking;

d) Không lưu lại tên đăng nhập và mã khóa bí mật, mã PIN trên các trình duyệt;

đ) Thoát khỏi phần mềm ứng dụng Online Banking khi không sử dụng;

e) Nhận dạng và hành động xử lý một số tình huống lừa đảo, giả mạo trang tin điện tử, phần mềm ứng dụng Online Banking;

g) Cài đặt đầy đủ các bản vá lỗ hổng bảo mật của hệ điều hành, phần mềm ứng dụng Mobile Banking; cài đặt phần mềm phòng chống mã độc và cập nhật mẫu nhận diện mã độc mới nhất trên thiết bị cá nhân sử dụng để giao dịch Online Banking;

h) Lựa chọn các giải pháp xác thực có mức độ an toàn, bảo mật phù hợp với nhu cầu của khách hàng về hạn mức giao dịch;

i) Cảnh báo các rủi ro liên quan đến việc sử dụng dịch vụ Online Banking;

k) Không sử dụng các thiết bị di động đã bị phá khóa để tải và sử dụng phần mềm Online Banking, phần mềm tạo OTP;

l) Không cài đặt các phần mềm lạ, không rõ nguồn gốc;

m) Thông báo kịp thời cho đơn vị khi phát hiện các giao dịch bất thường;

n) Thông báo ngay cho đơn vị các trường hợp: mất, thất lạc, hư hỏng thiết bị tạo OTP, số điện thoại nhận tin nhắn SMS, thiết bị lưu trữ khóa bảo mật tạo chữ ký số; bị lừa đảo hoặc nghi ngờ bị lừa đảo; bị tin tặc hoặc nghi ngờ bị tin tặc tấn công.

3. Đơn vị phải cung cấp cho khách hàng thông tin về đầu mối tiếp nhận thông tin, số điện thoại đường dây nóng và chỉ dẫn cho khách hàng quy trình, cách thức phối hợp xử lý các lỗi và sự cố trong quá trình sử dụng dịch vụ.

4. Đơn vị phải giải thích cho khách hàng về những trường hợp cụ thể đơn vị sẽ liên lạc với khách hàng, cách thức, phương tiện liên lạc trong quá trình khách hàng sử dụng dịch vụ.

5. Đơn vị không gửi tin nhắn, thư điện tử cho khách hàng có nội dung chứa đường dẫn truy cập các trang điện tử, trừ trường hợp theo yêu cầu của khách hàng.

## Điều 20. Bảo mật thông tin khách hàng

Đơn vị phải áp dụng các biện pháp bảo đảm an toàn, bảo mật cơ sở dữ liệu khách hàng, tối thiểu bao gồm:

1. Dữ liệu cá nhân của khách hàng phải được bảo đảm an toàn, bảo mật theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

2. Thông tin xác thực khách hàng bao gồm mã khóa bí mật, mã PIN, dấu hiệu sinh trắc học của khách hàng khi lưu trữ phải áp dụng các biện pháp mã hóa hoặc che dấu để bảo đảm tính bí mật.

3. Thiết lập quyền truy cập đúng chức năng, nhiệm vụ cho nhân sự thực hiện nhiệm vụ truy cập dữ liệu cá nhân khách hàng; có biện pháp giám sát mỗi lần truy cập.

4. Có biện pháp quản lý truy cập, tiếp cận các thiết bị, phương tiện lưu trữ dữ liệu cá nhân của khách hàng để phòng chống nguy cơ lộ, lọt dữ liệu.

# Chương III

# ĐIỀU KHOẢN THI HÀNH

## Điều 21. Chế độ báo cáo

Các đơn vị cung cấp dịch vụ Online Banking có trách nhiệm gửi báo cáo bằng văn bản về Ngân hàng Nhà nước Việt Nam (Cục Công nghệ thông tin) như sau:

1. Báo cáo cung cấp dịch vụ Online Banking:

a) Thời hạn gửi báo cáo: Tối thiểu 10 ngày làm việc trước khi cung cấp chính thức dịch vụ Online Banking;

b) Nội dung báo cáo:

(i) Địa chỉ trang tin điện tử hoặc hoặc kho ứng dụng cung cấp dịch vụ;

(ii) Các sản phẩm, dịch vụ hiện đang cung cấp;

(iii) Ngày cung cấp chính thức;

(iv) Đơn vị cung cấp sản phẩm hệ thống Online Banking;

(v) Bên thứ ba được thuê hoặc cùng hợp tác xây dựng, vận hành hệ thống Online Banking; các hoạt động liên quan đến hệ thống Online Banking có sự tham gia của bên thứ ba và hình thức tham gia của các bên thứ ba này;

(vi) Các giải pháp xác thực áp dụng với từng loại khách hàng, loại giao dịch và hạn mức giao dịch;

(vii) Các tài liệu khác về hạ tầng công nghệ thông tin và truyền thông, nhân lực, quy trình kỹ thuật nghiệp vụ, các phương án xử lý rủi ro và các nội dung liên quan khác theo quy định tại Chương II của Thông tư này.

2. Báo cáo đột xuất:

a) Khi xảy ra các sự cố mất an toàn hoặc ảnh hưởng đến hoạt động của hệ thống Online Banking, trong vòng 05 ngày kể từ thời điểm phát sinh sự cố hoặc phát hiện sự cố, đơn vị phải gửi báo cáo theo nội dung sau:

(i) Thời gian, địa điểm phát sinh sự cố;

(ii) Mô tả sơ bộ về sự cố, tình trạng khi xảy ra sự cố;

(iii) Nguyên nhân sự cố;

(iv) Đánh giá rủi ro, ảnh hưởng đối với hệ thống Online Banking và các hệ thống khác có liên quan;

(v) Tình hình thiệt hại;

(vi) Các biện pháp đã thực hiện để khắc phục sự cố, ngăn chặn và phòng ngừa rủi ro;

(vii) Kiến nghị, đề xuất.

b) Các trường hợp báo cáo đột xuất khác theo yêu cầu của Ngân hàng Nhà nước.

## Điều 22. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước

1. Cục Công nghệ thông tin có trách nhiệm:

a) Theo dõi, tổng hợp báo cáo Thống đốc Ngân hàng Nhà nước tình hình thực hiện việc đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin cung cấp dịch vụ Online Banking của các đơn vị theo quy định tại Điều 20 Thông tư này;

b) Chủ trì, phối hợp với các đơn vị liên quan thuộc Ngân hàng Nhà nước xử lý các vướng mắc phát sinh trong quá trình triển khai thực hiện Thông tư này.

2. Cơ quan Thanh tra, giám sát ngân hàng có trách nhiệm kiểm tra, thanh tra, giám sát việc thi hành Thông tư này và xử lý các trường hợp vi phạm theo thẩm quyền.

## Điều 23. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày tháng năm 2024, trừ trường hợp quy định tại khoản 2, khoản 3 và khoản 4 Điều này.

2. Điểm b khoản 1 Điều 4, điểm b khoản 9 Điều 11 có hiệu lực thi hành kể từ ngày 01 tháng 07 năm 2025.

3. Khoản 1 Điều 10 có hiệu lực thi hành kể từ ngày 01 tháng 01 năm 2025 đối với các giao dịch thanh toán thẻ trực tuyến.

4. Điểm g khoản 6 Điều 7, khoản 7 Điều 7, khoản 4 Điều 8, khoản 1 Điều 10 có hiệu lực thi hành kể từ ngày 01 tháng 01 năm 2025 đối với các tổ chức tín dụng được kiểm soát đặc biệt.

5. Thông tư này bãi bỏ Thông tư số 35/2016/TT-NHNN ngày 29 tháng 12 năm 2016 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet; khoản 5 Điều 1 Thông tư số 24/2018/TT-NHNN ngày 28 tháng 9 năm 2018 của Thống đốc Ngân hàng Nhà nước Việt Nam sửa đổi, bổ sung, bãi bỏ một số điều của các Thông tư, văn bản có quy định về chế độ báo cáo định kỳ; Thông tư số 35/2018/TT-NHNN ngày 24 tháng 12 năm 2018 của Thống đốc Ngân hàng Nhà nước Việt Nam sửa đổi, bổ sung một số điều của Thông tư số 35/2016/TT-NHNN ngày 29 tháng 12 năm 2016 của Thống đốc Ngân hàng Nhà nước Việt Nam quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet.

## Điều 24. Tổ chức thực hiện

Chánh Văn phòng, Cục trưởng Cục Công nghệ thông tin và Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước Việt Nam, Giám đốc Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc Trung ương; Chủ tịch Hội đồng quản trị, Chủ tịch Hội đồng thành viên, Tổng giám đốc (Giám đốc) các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, các tổ chức cung ứng dịch vụ trung gian thanh toán, công ty thông tin tín dụng chịu trách nhiệm tổ chức thực hiện Thông tư này./.

|  |  |
| --- | --- |
| ***Nơi nhận***:  **-** Như Điều 24;  - Ban Lãnh đạo NHNN;  - Văn phòng Chính phủ;  - Bộ Tư pháp (để kiểm tra);  - Công báo;  - Lưu VP, PC, CNTT. | **KT. THỐNG ĐỐC**  **PHÓ THỐNG ĐỐC** |

**PHỤ LỤC 01: PHÂN LOẠI GIAO DỊCH THEO CÁC NHÓM LOẠI HÌNH GIAO DỊCH  
TRONG THANH TOÁN TRỰC TUYẾN**

*(kèm theo Thông tư số /2024/TT-NHNN ngày tháng năm 2024 của Thống đốc Ngân hàng Nhà nước)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Loại hình giao dịch** | **Giao dịch loại A** | **Giao dịch loại B** | **Giao dịch loại C** | **Giao dịch loại D** |
| **I** | **Khách hàng cá nhân** |  |  |  |  |
| 1 | Nhóm I.1:  - Các giao dịch tra cứu thông tin.  - Chuyển tiền trong cùng ngân hàng, cùng chủ tài khoản. | Tất cả các giao dịch. |  |  |  |
| 2 | Nhóm I.2:  - Các giao dịch thanh toán hàng hóa, dịch vụ hợp pháp được tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán cung cấp hoặc tại các đơn vị chấp nhận thanh toán do các tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán chịu trách nhiệm lựa chọn, thẩm định, giám sát và quản lý. | Giao dịch thỏa mãn điều kiện:  G + T ≤ 5 triệu VND. | Giao dịch thỏa mãn các điều kiện:  (i) G + T > 5 triệu VND.  (ii) G + T ≤ 100 triệu VND. | Giao dịch thỏa mãn các điều kiện:  (i) G + T > 100 triệu VND.  (ii) G + T ≤ 1,5 tỷ VND. | Giao dịch thỏa mãn điều kiện:  G + T > 1,5 tỷ VND. |
| 3 | Nhóm I.3:  - Chuyển tiền trong cùng ngân hàng, khác chủ tài khoản.  - Chuyển tiền liên ngân hàng trong nước.  - Chuyển tiền giữa các ví điện tử.  - Nạp tiền vào Ví điện tử.  - Rút tiền từ Ví điện tử. |  | Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 10 triệu VND.  (ii) G + Tksth ≤ 20 triệu VND. | Giao dịch thỏa mãn một trong các trường hợp sau:  1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 10 triệu VND.  (ii) G + Tksth > 20 triệu VND.  (iii) G + T ≤ 1,5 tỷ VND.  2. Trường hợp 2: Giao dịch thỏa mãn các điều kiện:  (i) G > 10 triệu VND.  (ii) G≤ 500 triệu VND.  (iii) G + T ≤ 1,5 tỷ VND. | Giao dịch thỏa mãn một trong các trường hợp sau:  1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 10 triệu VND.  (ii) G + Tksth > 20 triệu VND.  (iii) G + T > 1,5 tỷ VND.  2. Trường hợp 2: Giao dịch thỏa mãn các điều kiện:  (i) G > 10 triệu VND.  (ii) G≤ 500 triệu VND.  (iii) G + T > 1,5 tỷ VND.  3. Trường hợp 3: Giao dịch thỏa mãn điều kiện:  G > 500 triệu VND. |
| 4 | Nhóm I.4:  Chuyển tiền liên ngân hàng ra nước ngoài\*. |  |  | Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 200 triệu VND.  (ii) G + T ≤ 1 tỷ VND. | Giao dịch thỏa mãn một trong các trường hợp sau:  1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 200 triệu VND.  (ii) G + T > 1 tỷ VND.  2. Trường hợp 2: Giao dịch thỏa mãn điều kiện:  G > 200 triệu VND. |
| **II** | **Khách hàng tổ chức** |  |  |  |  |
| 1 | Nhóm II.1:  Các giao dịch tra cứu thông tin. | Tất cả các giao dịch. |  |  |  |
| 2 | Nhóm II.2:  Chuyển tiền trong cùng ngân hàng, cùng chủ tài khoản. |  | Tất cả các giao dịch. |  |  |
| 3 | Nhóm II.3:  - Chuyển tiền trong cùng ngân hàng, khác chủ tài khoản.  - Chuyển tiền liên ngân hàng trong nước.  - Các giao dịch thanh toán hàng hóa, dịch vụ hợp pháp được tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán cung cấp hoặc tại các đơn vị chấp nhận thanh toán do các tổ chức cung ứng dịch vụ thanh toán, trung gian thanh toán chịu trách nhiệm lựa chọn, thẩm định, giám sát và quản lý.  - Chuyển tiền giữa các ví điện tử.  - Nạp tiền vào Ví điện tử.  - Rút tiền từ Ví điện tử. |  |  | Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 1 tỷ VND.  (ii) G + T ≤ 10 tỷ VND. | Giao dịch thỏa mãn một trong các trường hợp sau:  1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 1 tỷ VND.  (ii) G + T > 10 tỷ VND.  2. Trường hợp 2: Giao dịch thỏa mãn điều kiện:  G > 1 tỷ VND. |
| 4 | Nhóm II.4:  Chuyển tiền liên ngân hàng ra nước ngoài\* |  |  | Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 500 triệu VND.  (ii) G + T ≤ 5 tỷ VND. | Giao dịch thỏa mãn một trong các trường hợp sau:  1. Trường hợp 1: Giao dịch thỏa mãn các điều kiện:  (i) G ≤ 500 triệu VND.  (ii) G + T > 5 tỷ VND.  2. Trường hợp 2: Giao dịch thỏa mãn điều kiện:  G > 500 triệu VND. |

***Ghi chú:***

G: Giá trị của giao dịch.

Tksth: Tổng giá trị các giao dịch loại A và loại B của từng nhóm loại hình giao dịch đã thực hiện của một tài khoản ngân hàng (*bao gồm giao dịch nạp tiền vào ví điện tử*) hoặc một ví điện tử (*không bao gồm giao dịch nạp tiền vào ví điện tử*). Tksth của một tài khoản ngân hàng/ví điện tử được tính giá trị bằng 0 tại thời điểm đầu ngày hoặc ngay sau khi tài khoản ngân hàng/ví điện tử đó có phát sinh giao dịch trong ngày sử dụng biện pháp xác thực cho giao dịch loại C hoặc loại D.

T: Tổng giá trị các giao dịch của từng nhóm loại hình giao dịch đã thực hiện trong ngày (của một tài khoản ngân hàng (*bao gồm giao dịch nạp tiền vào ví điện tử*) hoặc một ví điện tử (*không bao gồm giao dịch nạp tiền vào ví điện tử*)).

\*: Hạn mức quy đổi theo tỷ giá tại thời điểm thực hiện giao dịch.

Trường hợp giao dịch nạp tiền vào Ví điện tử: căn cứ theo phân loại giao dịch của tài khoản ngân hàng của khách hàng được liên kết với Ví điện tử.

**PHỤ LỤC 02: CÁC HÌNH THỨC XÁC THỰC GIAO DỊCH ĐIỆN TỬ**

**TRONG THANH TOÁN TRỰC TUYẾN**

*(kèm theo Thông tư số /2024/TT-NHNN ngày tháng năm 2024 của Thống đốc Ngân hàng Nhà nước)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Giao dịch[[1]](#footnote-1)** | **Hình thức xác thực giao dịch điện tử tối thiểu** | | |
| **Khách hàng cá nhân là người Việt Nam** | **Khách hàng cá nhân là người nước ngoài** | **Khách hàng tổ chức** |
| 1 | Giao dịch loại A | - Tên đăng nhập, mật khẩu hoặc mã PIN (trường hợp đã xác thực tại bước đăng nhập thì không bắt buộc phải xác thực tại bước thực hiện giao dịch). | - Tên đăng nhập, mật khẩu hoặc mã PIN (trường hợp đã xác thực tại bước đăng nhập thì không bắt buộc phải xác thực tại bước thực hiện giao dịch). | - Tên đăng nhập, mật khẩu hoặc mã PIN (trường hợp đã xác thực tại bước đăng nhập thì không bắt buộc phải xác thực tại bước thực hiện giao dịch). |
| 2 | Giao dịch loại B | - SMS OTP hoặc Voice OTP hoặc Email OTP.  - Hoặc Thẻ ma trận OTP.  - Hoặc Soft OTP/ Token OTP loại cơ bản.  - Hoặc hình thức xác thực qua hai kênh.  - Hoặc bằng dấu hiệu nhận dạng sinh trắc học của khách hàng gắn liền với thiết bị cầm tay thông minh[[2]](#footnote-2).  - Hoặc Soft OTP/Token OTP loại nâng cao.  - Hoặc theo chuẩn FIDO.  - Hoặc bằng chữ ký điện tử. | - SMS OTP hoặc Voice OTP hoặc Email OTP.  - Hoặc Thẻ ma trận OTP.  - Hoặc Soft OTP/ Token OTP loại cơ bản.  - Hoặc hình thức xác thực qua hai kênh.  - Hoặc bằng dấu hiệu nhận dạng sinh trắc học của khách hàng gắn liền với thiết bị cầm tay thông minh.  - Hoặc Soft OTP/Token OTP loại nâng cao.  - Hoặc theo chuẩn FIDO.  - Hoặc bằng chữ ký điện tử. | - SMS OTP hoặc Voice OTP hoặc Email OTP.  - Hoặc Thẻ ma trận OTP.  - Hoặc Token OTP loại cơ bản, không có chức năng xác thực người dùng sử dụng Token.  - Hoặc bằng dấu hiệu nhận dạng sinh trắc học của người đại diện hợp pháp, người phụ trách kế toán (nếu có) của khách hàng gắn liền với thiết bị cầm tay thông minh. |
| 3 | Giao dịch loại C | - Bằng dấu hiệu nhận dạng sinh trắc học của khách hàng: (i) khớp đúng với dữ liệu sinh trắc học được lưu trong chíp của thẻ căn cước công dân (CCCD) của khách hàng do cơ quan Công an cấp[[3]](#footnote-3); (ii) hoặc thông qua xác thực tài khoản định danh điện tử của khách hàng do hệ thống định danh và xác thực điện tử tạo lập[[4]](#footnote-4).  - Hoặc bằng dấu hiệu nhận dạng sinh trắc học của khách hàng khớp đúng với dữ liệu sinh trắc học được lưu trong cơ sở dữ liệu (CSDL) sinh trắc học về khách hàng đã thu thập và kiểm tra[[5]](#footnote-5), khuyến khích kết hợp với phương thức xác thực OTP gửi qua SMS/Voice hoặc Soft OTP/Token OTP. | - Bằng dấu hiệu nhận dạng sinh trắc học của khách hàng thông qua xác thực tài khoản định danh điện tử của khách hàng do hệ thống định danh và xác thực điện tử tạo lập[[6]](#footnote-6).  - Hoặc bằng dấu hiệu nhận dạng sinh trắc học của khách hàng khớp đúng với dữ liệu sinh trắc học được lưu trong cơ sở dữ liệu (CSDL) sinh trắc học về khách hàng đã thu thập và kiểm tra[[7]](#footnote-7), khuyến khích kết hợp với phương thức xác thực OTP gửi qua SMS/Voice hoặc Soft OTP/Token OTP. | - Soft OTP/Token OTP loại cơ bản, có chức năng xác thực người dùng sử dụng phần mềm, Token.  - Hoặc hình thức xác thực qua hai kênh.  - Hoặc bằng chữ ký điện tử. |
| 4 | Giao dịch loại D | Bằng dấu hiệu nhận dạng sinh trắc học của khách hàng: (i) khớp đúng với dữ liệu sinh trắc học được lưu trong chíp của thẻ CCCD của khách hàng do cơ quan Công an cấp3; (ii) hoặc thông qua xác thực tài khoản định danh điện tử của khách hàng do hệ thống định danh và xác thực điện tử tạo lập4; (iii) hoặc khớp đúng với dữ liệu sinh trắc học được lưu trong CSDL sinh trắc học về khách hàng đã thu thập và kiểm tra5, kết hợp một trong các hình thức xác thực sau:  - Soft OTP/Token OTP loại nâng cao.  - Hoặc theo chuẩn FIDO.  - Hoặc bằng chữ ký điện tử an toàn. | Bằng dấu hiệu nhận dạng sinh trắc học của khách hàng: (i) thông qua xác thực tài khoản định danh điện tử của khách hàng do hệ thống định danh và xác thực điện tử tạo lập6; (ii) hoặc khớp đúng với dữ liệu sinh trắc học được lưu trong CSDL sinh trắc học về khách hàng đã thu thập và kiểm tra7, kết hợp một trong các hình thức xác thực sau:  - Soft OTP/Token OTP loại nâng cao.  - Hoặc theo chuẩn FIDO.  - Hoặc bằng chữ ký điện tử an toàn. | - Soft OTP/Token OTP loại nâng cao.  - Hoặc theo chuẩn FIDO.  - Hoặc bằng chữ ký điện tử an toàn. |

**Ghi chú:**

* Hình thức xác thực giao dịch loại D có thể xác thực giao dịch loại A, B, C.
* Hình thức xác thực giao dịch loại C có thể xác thực giao dịch loại A, B.
* Hình thức xác thực giao dịch loại B có thể xác thực giao dịch loại A.

1. Phân loại giao dịch quy định tại Phụ lục 01 Thông tư này. [↑](#footnote-ref-1)
2. Trường hợp khách hàng đã đăng nhập ứng dụng Internet Banking/ Mobile Banking bằng dấu hiệu nhận dạng sinh trắc học gắn liền với thiết bị cầm tay thông minh (như điện thoại thông minh (smart phone), máy tính bảng) thì không áp dụng biện pháp xác thực này khi thực hiện giao dịch trong phiên đăng nhập đó. [↑](#footnote-ref-2)
3. Đơn vị phải triển khai giải pháp để xác thực chính xác thẻ CCCD của khách hàng là do cơ quan Công an cấp. [↑](#footnote-ref-3)
4. Tài khoản định danh điện tử, hệ thống định danh và xác thực điện tử theo quy định của pháp luật về định danh và xác thực điện tử. [↑](#footnote-ref-4)
5. Kiểm tra đảm bảo: (i) sự khớp đúng giữa dữ liệu nhận dạng sinh trắc học của khách hàng với dữ liệu sinh trắc học trong chíp của thẻ CCCD của khách hàng do cơ quan Công an cấp; (ii) hoặc sự khớp đúng giữa dữ liệu nhận dạng sinh trắc học của khách hàng thông qua xác thực tài khoản định danh điện tử của khách hàng do hệ thống định danh và xác thực điện tử tạo lập; (iii) hoặc khớp đúng thông qua gặp mặt trực tiếp với khách hàng cá nhân không phải làm CCCD gắn chíp theo quy định của pháp luật. [↑](#footnote-ref-5)
6. Tài khoản định danh điện tử, hệ thống định danh và xác thực điện tử được xác định theo quy định của pháp luật về định danh và xác thực điện tử. [↑](#footnote-ref-6)
7. Kiểm tra đảm bảo sự khớp đúng giữa dữ liệu nhận dạng sinh trắc học của khách hàng thông qua: (i) xác thực tài khoản định danh điện tử của khách hàng do hệ thống định danh và xác thực điện tử tạo lập; (ii) hoặc gặp mặt trực tiếp khách hàng. [↑](#footnote-ref-7)