|  |  |
| --- | --- |
| **NGÂN HÀNG NHÀ NƯỚC  VIỆT NAM** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc** |
| Số: /2016/TT-NHNN | *Hà Nội, ngày tháng năm 2016* |

**DỰ THẢO 2**

# 

# THÔNG TƯ

# Quy định về an toàn, bảo mật cho việc cung cấp dịch

# vụ ngân hàng trên Internet

*Căn cứ Luật Ngân hàng Nhà nước Việt Nam số 46/2010/QH12 ngày 16 tháng 6 năm 2010;*

*Căn cứ Luật các tổ chức tín dụng số 47/2010/QH12 ngày 16 tháng 6 năm 2010;*

*Căn cứ Luật Giao dịch điện tử số 51/2005/QH11 ngày 29 tháng 11 năm 2005;*

*Căn cứ Luật an toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015;*

*Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29 tháng 06 năm 2006;*

*Căn cứ Nghị định số 35/2007/NĐ-CP ngày 08 tháng 3 năm 2007 của Chính phủ về giao dịch điện tử trong hoạt động ngân hàng;*

*Căn cứ Nghị định số 26/2007/NĐ-CP ngày 25 tháng 2 năm 2007 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;*

*Căn cứ Nghị định số 101/2012/NĐ-CP ngày 22 tháng 11 năm 2012 của Chính phủ về thanh toán không dùng tiền mặt;*

*Căn cứ Nghị định số 80/2016/NĐ-CP ngày 01 tháng 07 năm 2016 của Chính phủ về việc sửa đổi bổ sung một số điều của Nghị định 101/2012/NĐ-CP ngày 22 tháng 11 năm 2012 của Chính phủ về thanh toán không dùng tiền mặt;*

*Căn cứ Nghị định số 156/2013/NĐ-CP ngày 11 tháng 11 năm 2013 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;*

Ngân hàng Nhà nước Việt Nam quy định về an toàn, bảo mật hệ thống công nghệ thông tin cho việc cung cấp dịch vụ ngân hàng trên Internet như sau:

## 

## Chương I. QUY ĐỊNH CHUNG

### Phạm vi điều chỉnh và đối tượng áp dụng

* 1. Thông tư này quy định các yêu cầu đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin cho việc cung cấp dịch vụ ngân hàng trên Internet.
  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 cung cấp dịch vụ ngân hàng trên Internet tại Việt Nam (sau đây gọi chung là đơn vị).

### Giải thích từ ngữ và thuật ngữ

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

1. Dịch vụ ngân hàng trên Internet (Internet Banking) là các dịch vụ ngân hàng và dịch vụ trung gian thanh toán được cung cấp thông qua mạng Internet, bao gồm:

a) Tra cứu thông tin về đơn vị cung cấp dịch vụ và các dịch vụ của đơn vị.

b) Tra cứu thông tin khách hàng, tài khoản, truy vấn số dư và các thông tin khác của khách hàng.

c) Thực hiện các giao dịch tài chính như dịch vụ về tài khoản, chuyển khoản, cấp tín dụng, thanh toán qua tài khoản, dịch vụ về thẻ, thanh toán qua thẻ.

1. *Hệ thống Internet 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 Internet Banking.
2. *Khách hàng* là các tổ chức, cá nhân sử dụng dịch vụ Internet Banking.
3. *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.
4. *Xác thực hai yếu tố* là phương pháp xác thực yêu cầu hai yếu tố để chứng minh tính đúng đắn của một danh tính. Xác thực hai yếu tố dựa trên những thông tin mà người dùng biết (số PIN, mật khẩu) cùng với những gì mà người dùng có (thẻ thông minh, thiết bị token, ma trận lưới ngẫu nhiên …) để xác minh danh tính.
5. *Tài khoản đặc quyền* là tài khoản truy cập vào hệ thống công nghệ thông tin nhằm thực hiện các công việc đặc biệt hoặc truy cập vào dữ liệu nhạy cảm. Tài khoản đặc quyền thường sử dụng cho việc cấu hình thiết bị, quản trị hệ thống, quản trị hệ điều hành, quản trị cơ sở dữ liệu hoặc quản trị ứng dụng nghiệp vụ.
6. *Mã hóa điểm đầu đến điểm cuối (end to end encryption)* là cơ chế mã hoá 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.

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

1. Hệ thống cung cấp dịch vụ Internet Banking được xếp hạng là hệ thống công nghệ thông tin quan trọng và tuân thủ 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.
2. Đảm bảo bí mật thông tin khách hàng; tính toàn vẹn dữ liệu giao dịch khách hàng và mọi giao dịch tài chính củakhách hàng phải được xác thực tối thiểu hai yếu tố.
3. Đảm bảo tính sẵn sàng của hệ thống công nghệ thông tin để cung cấp dịch vụ Internet Banking một cách liên tục.
4. Bố trí nhân lực thực hiện việc quản trị, giám sát, vận hành hệ thống công nghệ thông tin và hỗ trợ khách hàng trong quá trình cung cấp dịch vụ Internet Banking.
5. Thực hiện kiểm tra, đánh giá an ninh, bảo mật hệ thống công nghệ thông tin Internet Banking theo định kỳ hàng năm.
6. Xác định rủi ro, có biện pháp phòng ngừa, xử lý rủi ro trong cung cấp dịch vụ Internet Banking.
7. Các trang thiết bị hạ tầng kỹ thuật công nghệ thông tin cung cấp dịch vụ Internet Banking phải có bản quyền, nguồn gốc, xuất xứ rõ ràng; trường hợp không còn hỗ trợ của nhà sản xuất, không có khả năng nâng cấp để cài đặt phần mềm phiên bản mới đơn vị phải có kế hoạch nâng cấp, thay thế theo thông báo của nhà sản xuất.

## 

## Chương II. CÁC QUY ĐỊNH CỤ THỂ

## Mục 1

## HỆ THỐNG HẠ TẦNG KỸ THUẬT CÔNG NGHỆ THÔNG TIN

### Hệ thống mạng, truyền thông

1. Chia tách hệ thống mạng thành các phân vùng, tối thiểu gồm: phân vùng kết nối Internet, phân vùng trung gian giữa mạng nội bộ và mạng Internet (DMZ), phân vùng người dùng (LAN), phân vùng quản trị, phân vùng máy chủ (server farm). Đối với các máy tính phục vụ cho việc cung cấp thông tin phải được đặt trong phân vùng DMZ. Các máy chủ lưu trữ, xử lý dữ liệu phải được đặt trong phân vùng máy chủ. Máy tính của người sử dụng, bao gồm cả nhân viên của đơn vị không phải là người quản lý tài khoản đặc quyền không được kết nối trực tiếp vào phân vùng máy chủ.
2. Trang bị các giải pháp an ninh bảo mật cho hệ thống Internet Banking, tối thiểu gồm: thiết bị tường lửa (Firewall); phòng chống vi rút; phòng chống tấn công từ chối dịch vụ; tường lửa bảo vệ lớp ứng dụng (Application Firewall) và phòng chống tấn công xâm nhập (IDS/IPS).
3. Dữ liệu nhạy cảm không được lưu trữ tại phân vùng kết nối Internet và phân vùng DMZ.
4. Kết nối từ bên ngoài vào hệ thống Internet Banking phải thông qua phân vùng DMZ để kiểm soát an ninh, bảo mật.
5. Thiết lập chính sách hạn chế tối đa các dịch vụ, cổng kết nối vào hệ thống công nghệ thông tin cung cấp dịch vụ Internet Banking.
6. Kiểm tra chính sách an ninh bảo mật; quyền truy cập; các kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào hệ thống mạng tối thiểu ba tháng một lần.
7. Không cho phép kết nối từ mạng không dây đến môi trường vận hành Internet Banking.
8. Hạn chế kết nối từ xa để thực hiện công tác quản trị hệ thống. Trường hợp bắt buộc phải kết nối từ xa vào vùng máy chủ, đơn vị phải sử dụng giao thức truyền thông được mã hóa và không lưu mã khóa bí mật tại các phần mềm tiện ích.
9. Kết nối từ Internet vào hệ thống mạng nội bộ để thực hiện công tác quản trị hệ thống phải được tuân thủ các quy tắc sau:

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

b) Phải sử dụng giao thức truyền thông được mã hóa.

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

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

1. Đường truyền kết nối Internet phải đảm bảo tính sẵn sàng và tối thiểu phải kết nối từ 2 nhà cung cấp dịch vụ khác nhau.11.
2. Trang bị giải pháp đảm bảo an toàn bảo mật giữa các phân vùng mạng: giữa các phân vùng mạng khác nhau phải có thiết bị tường lửa hoặc thiết bị phòng chống xâm nhập.

### 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) Có tính năng sẵn sàng cao: Hệ thống Internet Banking phải có máy chủ dự phòng tại chỗ.

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

1. Yêu cầu đối với phần mềm hệ thống

a) Kiểm tra, cập nhật các phiên bản vá lỗi kịp thời theo khuyến cáo của nhà sản xuất và tối thiểu sáu tháng một lần.

b) 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.

### 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. Rà soát, cập nhật các bản vá, các bản sửa lỗi hệ quản trị cơ sở dữ liệu tối thiểu sáu tháng một lần hoặc ngay sau khi có khuyến cáo của nhà cung cấp.
3. Hệ thống phải có cơ sở dữ liệu dự phòng tại Trung tâm dự phòng thảm họa. Cơ sở dữ liệu dự phòng phải được cập nhật không quá một giờ so với cơ sở dữ liệu chính thức. Cơ sở dữ liệu phải được sao lưu định kỳ hàng ngày. Các bản sao lưu phải được quản lý, cất giữ an toàn.
4. 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.

### Phần mềm ứng dụng

1. Các yêu cầu an toàn, bảo mật của nghiệp vụ phải được xác định trước và tổ chức, triển khai trong quá trình phát triển phần mềm: phân tích, thiết kế, kiểm thử, vận hành chính thức và bảo trì. Các tài liệu về an toàn, bảo mật của phần mềm phải được hệ thống hóa và lưu trữ, sử dụng theo chế độ “Mật”.
2. Kiểm soát chương trình nguồn

a) Kiểm tra mã nguồn, nhằm loại trừ các đoạn mã độc hại, các lỗ hổng bảo mật (back-door).

b) Chỉ định cụ thể các cá nhân quản lý chương trình nguồn của hệ thống ứng dụng Internet Banking.

c) Việc truy cập tới chương trình nguồn phải được người có thẩm quyền phê duyệt và được theo dõi, ghi nhật ký.

d) Chương trình nguồn phải được lưu trữ an toàn tại ít nhất hai địa điểm tách biệt.

đ) Trường hợp không được bàn giao chương trình 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.

1. Kiểm tra thử nghiệm phần mềm ứng dụng

a) Lập và phê duyệt kế hoạch, kịch bản thử nghiệm cho các ứng dụng Internet 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: Injection (SQL, Xpath, LDAP…), Cross-site Scripting (XSS), Cross-site Request Forgery (XSRF), Brute-Force.

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.

e) Việc sử dụng dữ liệu trong quá trình thử nghiệm phải có biện pháp phòng ngừa tránh bị lợi dụng hoặc gây nhầm lẫn.

1. Trước khi triển khai phần mềm ứng dụng mới, 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.
2. Quản lý và nâng cấp phiên bản phần mềm ứng dụng

a) Phân tích đánh giá ảnh hưởng của việc thay đổi đối với hệ thống hiện tại và các hệ thống có liên quan khác của đơn vị cho mỗi yêu cầu thay đổi phần mềm.

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

c) Thông tin về các phiên bản, thời gian cập nhật, người cập nhật các phiên bản phải được lưu lại.

d) Mỗi phiên bản được nâng cấp phải được kiểm tra thử nghiệm các tính năng an toàn, bảo mật, mức độ rủi ro và tính ổn định trước khi triển khai chính thức.

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

e) Các phiên bản phần mềm sau khi thử nghiệm thành công phải được quản lý chặt chẽ; tránh bị sửa đổi bất hợp pháp và sẵn sàng cho việc triển khai.

g) Có các chỉ dẫn rõ ràng về nội dung thay đổi, hướng dẫn cập nhật phần mềm, các thông tin liên quan khác và phải được người có thẩm quyền phê duyệt trước khi triển khai phiên bản mới cho khách hàng.

1. Các tính năng bắt buộc của phần mềm ứng dụng

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) Đảm bảo 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) Có cơ chế kiểm soát phiên giao dịch và thời gian truy cập website, ứng dụng. Trường hợp người sử dụng không thao tác trong một khoảng thời gian do đơn vị quy định nhưng không quá năm phút, hệ thống tự động ngắt phiên giao dịch hoặc áp dụng các biện pháp bảo vệ khác.

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

### Phần mềm trên thiết bị di động

Phần mềm Internet Banking trên thiết bị di động phải đảm bảo tuân thủ các quy định tại Điều 7 Thông tư này và các yêu cầu sau:

1. Chương trình nguồn phải được áp dụng các biện pháp bảo vệ để hạn chế dịch ngược.
2. Phần mềm dùng để tạo OTP phải sử dụng mã khóa do đơn vị cung cấp để kích hoạt trước khi sử dụng. Một mã khóa kích hoạt chỉ được sử dụng cho một thiết bị di động.
3. Khi truy cập phần mềm phải được xác thực. Trường hợp xác thực sai liên tiếp quá số lần do đơn vị quy định, nhưng không được quá năm lần, phần mềm phải tự động khoá tạm thời không cho khách hàng tiếp tục sử dụng.

### Hệ thống quản trị, giám sát hoạt động của hệ thống Internet Banking

1. Có hệ thống giám sát, theo dõi hoạt động của hệ thống Internet Banking.
2. Đơn vị phải xây dựng các tiêu chí để xác định các giao dịch đáng ngờ, bất thường và có phần mềm theo dõi.
3. Có phòng điều khiển để thực hiện việc quản trị, giám sát, theo dõi hoạt động của hệ thống Internet Banking đáp ứng yêu cầu sau:

a) Nhân sự ra vào phòng điều khiển phải được người có thẩm quyền phê duyệt.

b) Truy cập hệ thống để thực hiện công tác quản trị, vận hành và bảo trì phải được thực hiện thông qua các thiết bị đặt tại phòng điều khiển. Trường hợp cần truy cập từ xa hoặc trực tiếp trên thiết bị phải được người có thẩm quyền phê duyệt.

c) Truy cập từ bên ngoài vào các thiết bị đặt tại phòng điều khiển phải áp dụng các biện pháp xác thực hai yếu tố.

## Mục 2

## XÁC THỰC GIAO DỊCH TRONG DỊCH VỤ INTERNET BANKING

### Xác thực khách hàng truy cập dịch vụ Internet Banking

1. Việc truy cập vào tài khoản người dùng phải được xác thực tối thiểu bằng tên đăng nhập và mã khóa bí mật 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) Mã khóa bí mật phải có độ dài tối thiểu sáu ký tự, bao gồm các ký tự chữ và số, có chứa chữ hoa và chữ thường hoặc các ký tự đặc biệt.

1. Phần mềm ứng dụng phải có tính năng bắt buộc khách hàng thay đổi mã khóa bí mật ngay lần đăng nhập đầu tiên; khóa tài khoản truy cập trong trường hợp khách hàng nhập sai mã khóa bí mật liên tiếp quá số lần do đơn vị quy định, nhưng không được quá năm lần. Chỉ mở khóa tài khoản khi khách hàng yêu cầu mở tại quầy giao dịch.

### Hạn mức giao dịch tài chính đối với khách hàng cá nhân

1. Giao dịch loại A: Các giao dịch tài chính có số tiền dưới 50.000.000 (năm mươi triệu) đồng.
2. Giao dịch loại B: Các giao dịch tài chính có số tiền dưới 200.000.000 (hai trăm triệu) đồng.
3. Giao dịch loại C: Các giao dịch tài chính có số tiền dưới 500.000.000 (năm trăm triệu) đồng.
4. Giao dịch loại D: Các giao dịch tài chính có số tiền từ 500.000.000 (năm trăm triệu) đồng trở lên.

**Điều 12. Hạn mức giao dịch tài chính đối với khách hàng tổ chức**

Giao dịch loại B: các giao dịch tài chính có số tiền dưới 500.000.000 (năm trăm triệu) đồng.

Giao dịch loại C: các giao dịch tài chính có số tiền dưới 1.500.000.000 (một tỷ năm trăm triệu) đồng.

Giao dịch loại D: các giao dịch tài chính có số tiền trên 1.500.000.000 (một tỷ năm trăm triệu) đồng.

### Điều 13. Yêu cầu xác thực theo loại giao dịch

1. Giao dịch loại A: tối thiểu áp dụng một trong các giải pháp xác thực sau:

a) Sử dụng OTP được tạo từ ma trận lưới ngẫu nhiên.

b) Sử dụng OTP gửi qua tin nhắn SMS hoặc thư điện tử.

1. Giao dịch loại B: tối thiểu áp dụng một trong các giải pháp xác thực sau:

a) Sử dụng OTP được tạo từ thiết bị (OTP token).

b) Sử dụng OTP được tạo từ phần mềm cài đặt trên thiết bị di động.

1. Giao dịch loại C: áp dụng giải pháp xác thực sau:

~~a) Sử dụng OTP có chức năng ký giao dịch được tạo bởi thiết bị (token) hoặc phần mềm (cài trên thiết bị di động) từ mã giao dịch do hệ thống ứng dụng Internet Banking thông báo.~~

Sử dụng giải pháp xác thực hai chiều: hệ thống gửi thông tin về giao dịch đến thiết bị di động của khách hàng để khách hàng xác nhận thực hiện hoặc không thực hiện giao dịch.

1. Giao dịch loại D: tối thiểu áp dụng một trong các giải pháp sau:

a) Sử dụng OTP có chức năng ký giao dịch được tạo bởi thiết bị (token) hoặc phần mềm (cài trên thiết bị di động) từ mã giao dịch do hệ thống ứng dụng Internet Banking thông báo.

b) Chữ ký số.

c) Dấu hiệu nhận dạng sinh trắc học của khách hàng: Tĩnh mạch ngón tay hoặc bàn tay, mống mắt, giọng nói, khuôn mặt.

~~d) Sử dụng giải pháp xác thực hai chiều: hệ thống gửi thông tin về giao dịch đến thiết bị di động của khách hàng để khách hàng xác nhận thực hiện hoặc không thực hiện giao dịch~~

5. Giải pháp xác thực cho giao dịch loại D có thể sử dụng xác thực giao dịch loại C, B, A. Giải pháp xác thực cho giao dịch loại C có thể sử dụng xác thực giao dịch loại B, A. Giải pháp xác thực cho giao dịch loại B có thể sử dụng xác thực giao dịch loại A.

6. Đối với khách hàng là tổ chức, ngoài việc áp dụng giải pháp xác thực tương ứng với từng loại giao dịch được quy định tại Điều này, không được để một cá nhân làm toàn bộ các khâu từ khởi tạo đến phê duyệt một giao dịch.

### Điều 14. Yêu cầu đối với từng giải pháp xác thực giao dịch

1. Xác thực bằng OTP gửi qua tin nhắn SMS hoặc thư điện tử

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

b) Thời gian có hiệu lực tối đa của một OTP không quá 5 phút.

1. Xác thực bằng OTP được tạo từ phần mềm cài đặt trên thiết bị di động

a) Chỉ rõ đường dẫn trên website hoặc kho ứng dụng để khách hàng tải (download) phần mềm tạo OTP.

b) Cung cấp mã khóa bí mật để kích hoạt phần mềm tạo OTP cho khách hàng. Có giải pháp đảm bảo mã khóa bí mật chỉ có thể được sử dụng trên thiết bị của khách hàng đã đăng ký với đơn vị.

c) Phần mềm tạo OTP phải được kiểm soát truy cập. Trường hợp xác thực truy cập sai ba lần liên tiếp, phải tự động khoá tài khoản truy cập Internet Banking không cho khách hàng sử dụng.

d) Thời gian có hiệu lực tối đa của một OTP không quá 5 phút.

1. Xác thực bằng OTP được tạo từ thiết bị (OTP token)

a) Thời gian có hiệu lực tối đa của một OTP không quá 5 phút.

b) Thiết bị tạo OTP phải có tính năng yêu cầu người dùng đăng nhập trước khi tạo OTP.

1. Xác thực bằng chữ ký số: sử dụng chữ ký số và dịch vụ chứng thực chữ ký số của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng theo quy định của pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số.
2. Xác thực bằng dấu hiệu nhận dạng sinh trắc học: dấu hiệu nhận dạng sinh trắc học phải là dấu hiệu duy nhất gắn với mỗi khách hàng và không thể giả mạo.

## Mục 3

## QUẢN LÝ VẬN HÀNH

### Điều 15. Quản lý nhân sự quản trị, vận hành hệ thống Internet Banking

1. Có 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. Có nhân sự tiếp nhận thông tin, hỗ trợ khách hàng, kịp thời liên lạc với khách hàng khi phát hiện các giao dịch đáng ngờ, bất thường.
3. Nhân sự quản trị, giám sát và vận hành hệ thống Internet 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 Internet Banking phải được theo dõi, giám sát bởi bộ phận độc lập với bộ phận cấp phát tài khoản.

### Điều 16. Quản lý hoạt động của môi trường vận hành chính thức hệ thống Internet Banking

1. Không cài đặt, lưu trữ phần mềm phát triển ứng dụng, mã nguồn ứng dụng trên môi trường vận hành chính thức.
2. Các máy tính của nhân sự quản trị, giám sát và vận hành phải được đặt trong phân vùng mạng quản trị, được cài đặt phần mềm phòng chống vi rút và phải thiết lập chính sách tự động khóa màn hình sau một khoảng thời gian không sử dụng do đơn vị quy định, nhưng không quá 5 phút.
3. Thiết lập chính sách cấm truy cập Internet đối với các máy tính của nhân sự quản trị, giám sát và vận hành.

### Điều 17. Quản lý lỗ hổng, điểm yếu về mặt kỹ thuật

1. Có biện pháp phòng, chống, dò tìm phát hiện các thay đổi của website, ứng dụng Internet Banking.
2. Thiết lập cơ chế phát hiện, phòng chống xâm nhập, tấn công mạng vào hệ thống Internet 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. Rà soát, kiểm tra việc cập nhật các bản vá lỗi của phần mềm hệ thống, hệ quản trị cơ sở dữ liệu và phần mềm ứng dụng tối thiểu ba tháng một lần.
5. Đánh giá an ninh bảo mật đối với hệ thống Internet Banking tối thiểu mỗi năm một lần. Tổ chức thực hiện diễn tập tấn công thử nghiệm để kiểm tra, đánh giá mức độ đảm bảo an ninh của hệ thống.

### Điều 18. Quản lý sự cố bảo mật thông tin

Có biện pháp ghi nhận, theo dõi và xử lý các sự cố an ninh thông tin. Định kỳ ba tháng một lần đánh giá, tìm nguyên nhân và chủ động thực hiện các biện pháp phòng tránh tái diễn.

### Điều 19. Đảm bảo hoạt động liên tục

1. Xây dựng hệ thống dự phòng thảm họa cho hệ thống vận hành chính thức, đảm bảo có thể thay thế hệ thống chính thức trong thời gian tối đa bốn giờ kể từ khi hệ thống chính thức ngừng hoạt động.
2. Phân tích, xác định các tình huống có thể gây mất an ninh thông tin và gián đoạn hoạt động của hệ thống Internet 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.
3. 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 2 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.
4. 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.
5. 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 KHÁCH HÀNG

### Điều 20. Thông tin về dịch vụ Internet Banking

1. Cung cấp thông tin về dịch vụ Internet Banking cho khách hàng trước khi đăng ký sử dụng dịch vụ, tối thiểu gồm:

a) Cách thức cung cấp dịch vụ: trên Internet, thiết bị di động, viễn thông. Cách thức truy cập dịch vụ Internet Banking ứng với từng phương tiện truy cập dịch vụ trên Internet, thiết bị di động, viễn thông.

b) Hạn mức giao dịch và các biện pháp xác thực giao dịch.

c) Điều kiện cần thiết về trang thiết bị khi sử dụng dịch vụ: thiết bị tạo OTP; số điện thoại di động/thư điện tử; chữ ký số/chứng thư số; thiết bị di động để cài đặt phần mềm.

d) Các rủi ro liên quan đến việc sử dụng dịch vụ Internet Banking.

1. Thông tin cho khách hàng về hợp đồng cung cấp, sử dụng dịch vụ Internet Banking, tối thiểu gồm:

a) Quyền lợi và nghĩa vụ của khách hàng sử dụng dịch Internet Banking.

b) Trách nhiệm của đơn vị trong bảo mật các thông tin cá nhân của khách hàng; cách thức đơn vị thu thập, sử dụng thông tin khách hàng; cam kết không bán, tiết lộ, rò rỉ các thông tin khách hàng.

c) Cam kết khả năng đảm bảo hoạt động liên tục của hệ thống Internet Banking.

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

### Điều 21. Hướng dẫn khách hàng sử dụng dịch vụ Internet Banking

1. Xây dựng quy trình, tài liệu hướng dẫn cài đặt, sử dụng các phần mềm, ứng dụng, thiết bị trong thực hiện các giao dịch Internet Banking. Cung cấp và hướng dẫn sử dụng các quy trình, tài liệu này cho khách hàng.
2. Hướng dẫn khách hàng thực hiện các biện pháp đảm bảo an toàn, bảo mật khi sử dụng dịch vụ Internet Banking, tối thiểu gồm các nội dung sau:

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

b) Cách thiết lập mã khóa bí mật và thay đổi mã khóa bí mật tài khoản truy cập theo định kỳ tối thiểu sáu tháng một lần hoặc khi bị lộ, nghi bị lộ.

c) Không dùng máy tính công cộng để truy cập, thực hiện giao dịch Internet Banking.

d) Không lưu lại tên đăng nhập và mã khóa bí mật trên các trình duyệt web.

đ) Thoát khỏi hệ thống ứng dụng Internet Banking khi không sử dụng.

e) Nhận dạng và hành động xử lý một số tình huống lừa đảo, giả mạo website.

g) Yêu cầu cài đặt, sử dụng phần mềm diệt vi rút trên thiết bị cá nhân sử dụng để giao dịch Internet 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 tài chính.

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

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

1. Cung cấp cho khách hàng đầu mối tiếp nhận thông tin, số điện thoại đường dây nóng. Chỉ dẫn khách hàng phối hợp, trao đổi thông tin hai chiều:

a) Thông báo cho đơn vị phối hợp xử lý các lỗi và sự cố trong quá trình sử dụng dịch vụ.

b) Thông báo kịp thời cho đơn vị khi phát hiện các giao dịch bất thường, đáng ngờ.

c) 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 khoá 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.

### Điều 22. Bảo mật thông tin và đảm bảo quyền lợi khách hàng

1. Áp dụng các biện pháp đảm bảo an toàn, bảo mật cơ sở dữ liệu khách hàng. Dữ liệu nhạy cảm của khách hàng khi lưu trữ, truyền trên mạng Internet phải được mã hóa hoặc che dấu.
2. Thiết lập quyền truy cập vừa đủ cho nhân sự thực hiện nhiệm vụ khi truy cập dữ liệu khách hàng; có biện pháp giám sát mỗi lần truy cập.
3. Có biện pháp quản lý truy cập, tiếp cận các thiết bị, phương tiện lưu trữ dữ liệu về thông tin khách hàng; ngăn chặn rò rỉ, lộ lọt dữ liệu.

## Chương III. ĐIỀU KHOẢN THI HÀNH

### Điều 23. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 30/09/2017 và thay thế Thông tư 29/2011/TT-NHNN ngày 21/9/2011 của Thống đốc Ngân hàng Nhà nước Việt Nam về việc ban hành Quy định việc đảm bảo an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet.
2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị phản ánh kịp thời về Ngân hàng Nhà nước để xem xét, bổ sung, sửa đổi.

### Điều 24. Trách nhiệm thi hành

1. Cục Công nghệ tin học có trách nhiệm:

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

~~b) Hàng năm lập kế hoạch và kiểm tra việc thực hiện Thông tư này tại các đơn vị.~~

c) 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.

1. Cơ quan Thanh tra, giám sát ngân hàng có trách nhiệm phối hợp với Cục Công nghệ tin học kiểm tra, giám sát việc thi hành Thông tư này và xử lý vi phạm hành chính đối với hành vi vi phạm theo quy định của pháp luật.
2. Chánh Văn phòng, Cục trưởng Cục Công nghệ tin học và Thủ trưởng các đơn vị thuộc Ngân hàng Nhà nước Việt Nam, Giám đốc Ngân hàng Nhà nước chi nhánh các 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 cung cấp dịch vụ Internet Banking chịu trách nhiệm thi hành Thông tư này./.

|  |  |
| --- | --- |
| ***Nơi nhận:*** - Như Khoản 3 Điều 24; - Ban Lãnh đạo NHNN; - Văn phòng Chính phủ; - Bộ Tư pháp (để kiểm tra); - Công báo; - Lưu: VP, CNTH, PC. | **THỐNG ĐỐC** |