NGÂN HÀNG NHÀ NƯỚC VIỆT NAM

NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 35/2016/TT-NHNN	*Hà Nội, ngày 29 tháng 12 năm 2016*

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 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 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;

Theo đề nghị của Cục trưởng Cục Công nghệ tin học,

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 ngân hàng trên Internet.

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 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 tại Việt Nam (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 ngân hàng trên Internet (Internet Banking)* là các dịch vụ ngân hàng và dịch vụ trung gian thanh toán được các đơn vị cung cấp thông qua mạng Internet.

2. *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.

3. *Khách hàng* là các tổ chức, cá nhân sử dụng dịch vụ Internet Banking.

4. *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 InternetBanking.

5. *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, mã khóa bí mật,…) cùng với những gì mà người dùng có (thẻ thông minh, thiết bị token, điện thoại di động…) hoặc những dấu hiệu sinh trắc học của người dùng để xác minh danh tính.

6. *Mã hóa điểm đầu đến điểm cuối (end to end encryption)* là cơ chế mã hóa 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.

Điều 3. 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 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 của khách hàng phải được xác thực tối thiểu hai yếu tố.

3. Đảm bảo tính sẵn sàng của hệ thống Internet Banking để cung cấp dịch vụ một cách liên tục.

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

5. Xác định rủi ro, có biện pháp phòng ngừa, xử lý rủi ro trong cung cấp dịch vụ Internet Banking.

6. 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
HẠ TẦNG KỸ THUẬT CỦA HỆ THỐNG INTERNET 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. Hệ thống mạng được chia tách thành các phân vùng, tối thiểu gồm: phân vùng kết nối Internet, phân vùng trung gian giữa mạng nội bộ và mạng Internet (phân vùng DMZ), phân vùng người dùng, phân vùng quản trị, phân vùng máy chủ. Các máy tính phục vụ cho việc cung cấp thông tin trên Internet phải được đặt trong phân vùng DMZ. Các máy chủ lưu trữ, xử lý dữ liệu phải được đặt trong 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; phòng chống vi rút; phòng chống tấn công từ chối dịch vụ; tường lửa bảo vệ lớp ứng dụng và phòng chống tấn công xâm nhập.

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 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 thiết lập kết nối từ mạng không dây đến môi trường vận hành hệ thống 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.

10. Đường truyền kết nối Internet phải đảm bảo tính sẵn sàng và tối thiểu phải kết nối từ hai nhà cung cấp dịch vụ khác nhau.

11. 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.

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) 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.

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 Internet Banking 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.

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 Internet Banking

1. Các yêu cầu an toàn, bảo mật phải được xác định trước và tổ chức, triển khai trong quá trình phát triển phần mềm ứng dụng: 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. Đơn vị phải kiểm soát mã nguồn phần mềm với các yêu cầu tối thiểu:

a) Kiểm tra mã nguồn, nhằm loại trừ các đoạn mã độc hại, các lỗ hổng bảo mật;

b) Chỉ định cụ thể các cá nhân quản lý mã nguồn của phần mềm ứng dụng Internet Banking;

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

d) Mã nguồn phải được lưu trữ an toàn tại ít nhất hai địa điểm tách biệt;

đ) 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. Đơn vị phải kiểm tra thử nghiệm phần mềm ứng dụng Internet Banking đáp ứng các yêu cầu tối thiểu sau:

a) Lập và phê duyệt kế hoạch, kịch bản thử nghiệm phần mềm 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.

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 và nâng cấp phiên bản phần mềm ứng dụng đáp ứng các yêu cầu sau:

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 ứng dụng;

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 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 ứng dụng sau khi thử nghiệm thành công phải được quản lý chặt chẽ; tránh bị sửa đổi trái phép 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 ứng dụng, 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.

6. 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 đối với việc hiển thị các mã khóa bí mật dùng để đăng nhập vào hệ thống;

đ) Đối với khách hàng là tổ chức, phần mềm ứng dụng được thiết kế để đảm bảo việc thực hiện giao dịch bao gồm tối thiểu hai bước: tạo, phê duyệt giao dịch và được thực hiện bởi tối thiểu hai người khác nhau.

Điều 8. Phần mềm ứng dụng trên thiết bị di động

Phần mềm ứng dụng Internet Banking trên thiết bị di động 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. Đơn vị phải chỉ rõ đường dẫn trên website hoặc kho ứng dụng để khách hàng tải và cài đặt phần mềm ứng dụng Internet Banking trên thiết bị di động.

2. Phần mềm ứng dụng phải được áp dụng các biện pháp bảo vệ để hạn chế dịch ngược.

3. Phần mềm ứng dụng phải xác thực người dùng khi truy cập. Trường hợp xác thực sai liên tiếp quá số lần do đơn vị quy định, nhưng không được quá năm lần, phần mềm ứng dụng phải tự động khóa tạm thời không cho khách hàng tiếp tục sử dụng.

Mục 2
XÁC THỰC GIAO DỊCH INTERNET BANKING

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

1. Khách hàng truy cập sử dụng dịch vụ Internet Banking 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. Thời gian hiệu lực của mã khóa bí mật tối đa 12 tháng.

2. Phần mềm ứng dụng Internet Banking 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.

Điều 10. Yêu cầu đối với các giải pháp xác thực giao dịch

1. Đơn vị phải đánh giá mức độ rủi ro của giao dịch theo từng loại khách hàng, loại giao dịch, hạn mức giao dịch để cung cấp giải pháp xác thực giao dịch phù hợp cho khách hàng lựa chọn. Hạn mức giao dịch không vượt quá hạn mức quy định của Thống đốc Ngân hàng Nhà nước trong từng thời kỳ.

2. Yêu cầu đối với giải pháp 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 biết được mục đích của OTP;

b) OTP có hiệu lực tối đa không quá 05 phút.

3. Yêu cầu đối với giải pháp xác thực bằng thẻ ma trận OTP:

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. Yêu cầu đối với giải pháp xác thực bằng OTP được tạo từ phần mềm cài đặt trên thiết bị di động:

a) Đơn vị phải chỉ rõ đường dẫn trên website hoặc kho ứng dụng để khách hàng tải và cài đặt phần mềm tạo OTP;

b) Phần mềm 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;

c) Phần mềm tạo OTP phải được kiểm soát truy cập. Trường hợp xác thực truy cập sai năm lần liên tiếp, phần mềm phải tự động khóa không cho khách hàng sử dụng tiếp;

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

5. Yêu cầu đối với giải pháp xác thực bằng OTP được tạo từ thiết bị (OTP token): OTP có hiệu lực tối đa không quá 02 phút.

6. Yêu cầu đối với giải pháp xác thực bằng chữ ký số: Đơn vị phải 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 hoạt động theo quy định của pháp luật về chữ ký số và dịch vụ chứng thực chữ ký số.

7. Yêu cầu đối với giải pháp 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 11. Quản lý nhân sự quản trị, vận hành hệ thống Internet 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 Internet Banking phải tham gia các khóa đào tạo cập nhật kiến thức an ninh, bảo mật hàng 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 12. Quản lý hoạt động của môi trường vận hành hệ thống Internet Banking

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

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 05 phút.

3. Đơn vị phải thiết lập chính sách cấm truy cập Internet đối với các máy tính của nhân sự quản trị, giám sát và vận hành.

Điều 13. 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 Internet Banking với các nội dung cơ bản sau:

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

1. Đơn vị phải thiết lập hệ thống giám sát, theo dõi hoạt động của hệ thống Internet Banking.

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.

3. Đơn vị phải bố trí phòng điều khiển tách biệt với khu vực làm việc chung 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.

Điều 15. Quản lý sự cố bảo mật thông tin

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

Điều 16. Đảm bảo hoạt động liên tục

Đơn vị phải xây dựng hệ thống dự phòng thảm họa, quy trình, kịch bản đảm bảo hoạt động liên tục cho hệ thống Internet 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 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.

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 Internet Banking

1. Đơn vị phải 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, 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.

2. Đơn vị phải 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 vụ 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 18. Hướng dẫn khách hàng sử dụng dịch vụ Internet 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 Internet 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 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 một năm 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 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;

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 ứng dụng Internet Banking, phần mềm tạo OTP.

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

m) 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.

Điều 19. Bảo mật thông tin khách hàng

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

1. 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 đúng chức năng, nhiệm vụ cho nhân sự thực hiện nhiệm vụ 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 để phòng chống nguy cơ lộ, lọt thông tin khách hàng.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 20. Chế độ báo cáo

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

1. Báo cáo cung cấp dịch vụ Internet Banking:

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

b) Nội dung báo cáo:

(i) Địa chỉ website 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 Internet Banking;

(v) Bên thứ ba được thuê hoặc cùng hợp tác xây dựng, vận hành hệ thống Internet Banking; các hoạt động liên quan đến hệ thống Internet 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 Internet 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 Internet 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.

3. Báo cáo năm:

Thời hạn và nội dung báo cáo theo quy định của Ngân hàng Nhà nước về chế độ báo cáo thống kê áp dụng đối với các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài.

Điều 21. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước

1. Cục Công nghệ tin học 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 Internet 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 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.

Điều 22. Hiệu lực thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 01/7/2017 và thay thế Thông tư số 29/2011/TT-NHNN ngày 21/9/2011 của Ngân hàng Nhà nước Việt Nam quy định về đảm bảo an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet.

Điều 23. Tổ chức thực hiện

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 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 chịu trách nhiệm tổ chức thực hiện Thông tư này./.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Nguyễn Kim Anh