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: 29/2011/TT-NHNN	*Hà Nội, ngày 21 tháng 9 năm 2011*

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 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 64/2001/NĐ-CP ngày 20 tháng 9 năm 2001 của Chính phủ về hoạt động thanh toán qua các tổ chức cung ứng dịch vụ thanh toán;

Căn cứ Nghị định số 26/2007/NĐ-CP ngày 25 tháng 02 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 96/2008/NĐ-CP ngày 26 tháng 8 năm 2008 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Ngân hàng Nhà nước Việt Nam;

Căn cứ Nghị định số 97/2008/NĐ-CP ngày 28 tháng 8 năm 2008 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin điện tử trên Internet;

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

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 cung cấp dịch vụ ngân hàng trên Internet (sau đây gọi chung là đơn vị cung cấp dịch vụ) tại Việt Nam.

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 (dịch vụ Internet Banking)*: là các dịch vụ ngân hàng được cung cấp thông qua mạng Internet, bao gồm:

a) Thông tin về đơn vị cung cấp dịch vụ và các dịch vụ của đơn vị;

b) Dịch vụ tra cứu thông tin như: tra cứu thông tin khách hàng, tài khoản, truy vấn số dư và các thông tin khác;

c) Thực hiện các giao dịch tài chính trực tuyến như: dịch vụ về tài khoản, chuyển khoản, cấp tín dụng, thanh toán qua tài khoản;

d) Các dịch vụ khác theo quy định của Ngân hàng nhà nước.

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 phục vụ cho việc quản lý và cung cấp dịch vụ ngân hàng trên Internet.

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

4. *Xác thực hai yếu tố*: là phương pháp xác thực yêu cầu hai yếu tố khác nhau để chứng minh tính đúng đắn của một danh tính. Xác thực hai yếu tố dựa trên những thông tin mà người dùng biết như mã số khách hàng, mật khẩu, cùng với những gì mà người dùng có như mật khẩu sử dụng một lần (OTP), ma trận lưới ngẫu nhiên, dấu hiệu sinh trắc học, hoặc các thiết bị hỗ trợ khác để chứng 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 hay quản trị ứng dụng nghiệp vụ (ví dụ như các tài khoản root, supervisors, system, administrator).

Điều 3. Nguyên tắc chung đối với việc cung cấp dịch vụ ngân hàng trên Internet của đơn vị cung cấp dịch vụ

1. Đảm bảo tính bí mật

a) Đảm bảo bí mật thông tin liên quan đến tài khoản, tiền gửi, tài sản gửi và các giao dịch của khách hàng theo quy định của pháp luật;

b) Mật khẩu khách hàng, khóa mã hóa và các mã khóa khác phải được mã hóa trong quá trình giao dịch, trên đường truyền và lưu trữ tại đơn vị cung cấp dịch vụ;

2. Đảm bảo tính sẵn sàng

a) Cam kết khả năng hoạt động liên tục của hệ thống Internet Banking một cách công khai, rõ ràng và được nêu rõ trong hợp đồng cung cấp dịch vụ với khách hàng. Cam kết này tối thiểu phải bao gồm cam kết về tổng thời gian dừng hệ thống trong năm, khoảng thời gian cung cấp dịch vụ trong ngày, thời gian phục hồi hệ thống sau khi gặp sự cố;

b) Đáp ứng đủ nguồn lực về hạ tầng công nghệ thông tin và nhân sự đảm bảo cung cấp dịch vụ Internet Banking liên tục đúng như cam kết của đơn vị cung cấp dịch vụ với khách hàng;

c) Xây dựng, ban hành và tuân thủ các quy trình của hệ thống Internet Banking;

d) Sử dụng các công cụ giám sát, theo dõi hiệu năng của hệ thống chính và hệ thống dự phòng đảm bảo hoạt động liên tục.

3. Đảm bảo tính toàn vẹn

a) Đảm bảo tính toàn vẹn của thông tin trong quá trình xử lý, lưu trữ và truyền nhận giữa đơn vị cung cấp dịch vụ và khách hàng;

b) Kết hợp các biện pháp an ninh về mặt hành chính và kỹ thuật trong:

- Truy cập vật lý;
- Truy cập lô gíc;
- Quá trình nhập, xử lý, truyền dẫn, kết xuất, lưu trữ, khôi phục dữ liệu.

4. Xác thực khách hàng và xác thực giao dịch

a) Đảm bảo xác thực và nhận dạng được khách hàng khi khách hàng truy cập và sử dụng dịch vụ Internet Banking;

b) Sử dụng xác thực hai yếu tố trên hệ thống Internet Banking khi thực hiện giao dịch thanh toán và các giao dịch quan trọng như: tạo kết nối giữa các tài khoản, đăng ký thanh toán cho bên thứ ba, thay đổi hạn mức giao dịch trong ngày, thay đổi thông tin tài khoản liên quan đến dữ liệu cá nhân của khách hàng (như địa chỉ cơ quan hoặc nhà riêng, số điện thoại liên lạc, địa chỉ thư điện tử và các thông tin khác nhằm xác thực khách hàng).

5. Bảo vệ khách hàng

a) Cung cấp đầy đủ thông tin về quyền lợi và nghĩa vụ của khách hàng trước khi ký kết hợp đồng cung cấp dịch vụ với khách hàng. Trong hợp đồng cung cấp dịch vụ phải nêu rõ việc đơn vị cung cấp dịch vụ đảm bảo các khoản nêu ra tại Điều này đối với khách hàng. Đơn vị cung cấp dịch vụ chịu trách nhiệm thực hiện đầy đủ các điều khoản thuộc trách nhiệm của mình nêu trong hợp đồng cung cấp dịch vụ ký kết với khách hàng;

b) Trong hợp đồng cung cấp dịch vụ, đơn vị cung cấp dịch vụ phải nêu rõ trách nhiệm bảo mật các thông tin cá nhân của khách hàng khi sử dụng dịch vụ Internet Banking; nêu rõ cách thức ngân hàng thu thập, sử dụng thông tin khách hàng, cam kết không bán, tiết lộ, rò rỉ các thông tin đó;

c) Có biện pháp đảm bảo an toàn, bảo mật trong trường hợp đơn vị cung cấp dịch vụ phân phối phần mềm cho khách hàng qua môi trường Internet;

d) Chịu trách nhiệm kiểm tra, cảnh báo và thực hiện các biện pháp phòng chống giả mạo website cung cấp dịch vụ Internet Banking của đơn vị cung cấp dịch vụ; đồng thời có trách nhiệm thông báo phương thức xác định website thật đến khách hàng.

Chương II
CÁC QUY ĐỊNH CỤ THỂ

Điều 4. Chính sách về an toàn, bảo mật hệ thống

Xây dựng, ban hành các quy định an toàn, bảo mật cho hệ thống Internet Banking phù hợp với quy định về an toàn, bảo mật hệ thống công nghệ thông tin của Nhà

nước, ngành Ngân hàng và quy chế an toàn bảo mật công nghệ thông tin của đơn vị. Định kỳ tối thiểu mỗi năm một lần, đơn vị phải rà soát, chỉnh sửa, hoàn thiện các quy định này đảm bảo sự phù hợp, đầy đủ và có hiệu quả của quy định.

Điều 5. Quản lý nguồn nhân lực

1. Lựa chọn đội ngũ cán bộ có đủ tư cách đạo đức, trình độ, năng lực đáp ứng được yêu cầu về chuyên môn nghiệp vụ và công nghệ khi phân công nhiệm vụ liên quan đến hệ thống Internet Banking.

2. Các nhiệm vụ quản trị hệ thống; phát triển, bảo trì phần mềm ứng dụng và vận hành hệ thống phải được phân công cho từng bộ phận, cá nhân khác nhau. Đảm bảo kiểm soát chéo và không một cá nhân nào có toàn quyền trên hệ thống hoặc có thể tự khởi tạo, can thiệp vào các giao dịch của hệ thống Internet Banking. Có quy định trách nhiệm và phân quyền rõ ràng cho từng nhóm bộ phận, cá nhân nêu trên. Tài khoản đặc quyền trên hệ thống Internet Banking phải được thiết kế để chỉ có thể truy cập được khi có khóa của ít nhất hai người và phải được kiểm soát chặt chẽ đối với mọi hoạt động của tài khoản này.

3. Có quy định cụ thể, rõ ràng và thực hiện đầy đủ công tác quản lý, giám sát nhân sự bên thứ ba khi truy cập vào hệ thống Internet Banking. Các yêu cầu về an toàn, bảo mật và thỏa thuận cần xác định rõ trong hợp đồng với bên thứ ba.

Điều 6. Mạng truyền thông

1. Có biện pháp phân tách các phân vùng mạng để đảm bảo kiểm soát được các truy cập hệ thống.

2. Có biện pháp phát hiện và phòng chống xâm nhập, phòng chống phát tán mã độc hại cho hệ thống.

3. Xây dựng và thực hiện phương án dự phòng cho các vị trí quan trọng có mức độ ảnh hưởng cao tới hệ thống mạng hoặc có khả năng gây tê liệt toàn bộ hệ thống mạng của đơn vị khi xảy ra sự cố.

4. Các kết nối không dây phải sử dụng các biện pháp xác thực đảm bảo an toàn.

5. Đảm bảo yêu cầu về băng thông đối với việc cung cấp dịch vụ Internet Banking.

6. Cập nhật các bản vá lỗi hệ thống, cập nhật cấu hình cho các thiết bị mạng và các thiết bị bảo mật tối thiểu sáu tháng một lần. Trong trường hợp phát hiện lỗi hệ thống phải thực hiện cập nhật ngay.

7. Các trang thiết bị mạng, an ninh, bảo mật, phần mềm chống vi rút, công cụ phân tích, quản trị mạng được cài đặt trong mạng của đơn vị phải có bản quyền và nguồn gốc, xuất xứ rõ ràng.

Điều 7. Phần cứng và phần mềm hệ thống

1. Đảm bảo có hạ tầng máy chủ và các thiết bị đi kèm phục vụ hệ thống Internet Banking (sau đây gọi là máy chủ Internet Banking) đủ công suất, đạt hiệu năng yêu cầu, đảm bảo tốc độ xử lý truy xuất đáp ứng yêu cầu của khách hàng sử dụng dịch vụ.

2. Yêu cầu đối với máy chủ Internet Banking

a) Có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo tính hoạt động liên tục;

b) Được đặt ở nơi được bảo vệ an toàn và được giám sát chặt chẽ;

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

3. Yêu cầu đối với phần mềm hệ thống:

a) Được rà soát, cập nhật các phiên bản vá lỗi phần mềm hệ thống theo khuyến cáo của nhà cung cấp tối thiểu sáu tháng một lần;

b) Lập danh mục các phần mềm được phép cài đặt trên máy chủ Internet Banking và định kỳ tối thiểu ba tháng một lần cập nhật, kiểm tra, đảm bảo tuân thủ danh mục này.

Điều 8. Phần mềm ứng dụng

1. Các yêu cầu chung

a) Các yêu cầu an toàn, bảo mật của nghiệp vụ phải được xác định trước và tổ chức, triển khai vào toàn bộ chu trình phát triển phần mềm từ khâu phân tích, thiết kế đến triển khai vận hành và bảo trì;

b) 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";.

c) Trước khi triển khai chương trình 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;

d) Phải xác định, thống kê được các hoạt động và giao dịch bất thường phát sinh trong hệ thống.

2. Kiểm tra thử nghiệm phần mềm ứng dụng

a) Lập và phê duyệt kế hoạch, kịch bản thử nghiệm cho các ứng dụng cung cấp dịch vụ 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 và các lỗ hổng bảo mật trong quá trình kiểm tra thử nghiệm hệ thống;

c) 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;

d) Kiểm tra thử nghiệm các tính năng an toàn, bảo mật phải được thực hiện trên các trình duyệt phổ biến như Internet Explorer, Mozilla Firefox, Google Chrome;

đ) Tiến hành thử nghiệm trên môi trường riêng biệt và không ảnh hưởng đến hoạt động bình thường của nghiệp vụ. Lập báo cáo kết quả thử nghiệm trình cấp có thẩm quyền phê duyệt trước khi đưa vào sử dụng;

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

3. Quản lý và nâng cấp phiên bản

a) Đối với mỗi yêu cầu thay đổi phần mềm, phải phân tích đánh giá ảnh hưởng

của việc thay đổi đối với các hệ thống hiện tại cũng như các nghiệp vụ và các hệ thống công nghệ thông tin có liên quan khác của đơn vị;

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

4. 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 Internet Banking;

c) Việc truy cập tới chương trình nguồn phải được sự phê chuẩn của cấp có thẩm quyền 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) Trong trường hợp đơn vị cung cấp dịch vụ mua phần mềm từ bên thứ ba mà không được bàn giao chương trình nguồn, đơn vị cung cấp dịch vụ phải yêu cầu bên thứ ba ký cam kết không có các đoạn mã độc hại trong phần mềm ứng dụng bàn giao cho đơn vị cung cấp dịch vụ.

Điều 9. An toàn cơ sở dữ liệu

1. Chỉ được sử dụng các hệ quản trị cơ sở dữ liệu có bản quyền và xuất xứ, nguồn gốc rõ ràng và đã được kiểm nghiệm qua thực tế hoạt động nghiệp vụ của các tổ chức tương tự trong hoặc ngoài nước.

2. Hệ quản trị cơ sở dữ liệu sử dụng cho hệ thống Internet Banking phải đáp ứng được yêu cầu hoạt động ổn định; xử lý, lưu trữ được khối lượng dữ liệu lớn theo yêu cầu nghiệp vụ; có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu.

3. 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.

4. Xây dựng phương án sao lưu, dự phòng đối với cơ sở dữ liệu, đảm bảo các hệ thống Internet Banking hoạt động liên tục khi xảy ra sự cố với cơ sở dữ liệu.

5. Thực hiện phân quyền và có quy định chặt chẽ với từng cá nhân truy cập đến cơ sở dữ liệu. Phải ghi nhật ký đối với các truy cập cơ sở dữ liệu, các thao tác đối với cấu hình cơ sở dữ liệu.

6. Có giải pháp ngăn chặn các hình thức tấn công cơ sở dữ liệu.

Điều 10. Mã hóa dữ liệu

1. Lựa chọn thuật toán mã hóa đáp ứng yêu cầu bảo đảm tính bí mật và khả năng xử lý của hệ thống Internet Banking.

2. Thuật toán mã hóa đang sử dụng phải được định kỳ mỗi năm một lần kiểm tra, đánh giá lại mức độ an toàn và xử lý kịp thời những yếu điểm nếu có.

3. Không để một cá nhân thực hiện toàn bộ quá trình tạo khóa mã hóa. Các khóa mã hóa phải được khởi tạo, thay đổi, phân phối, lưu trữ một cách an toàn.

4. Phải bảo đảm khôi phục được các thông tin đã mã hóa khi cần thiết.

5. Có những quy định chặt chẽ về việc thu hồi các khóa mã hóa, bao gồm cả việc hủy khóa và phục hồi khóa.

Điều 11. Quản lý nhật ký

1. Ghi nhật ký các sự kiện sau đối với hệ thống Internet Banking:

a) Quá trình truy cập hệ thống;

b) Các thao tác cấu hình hệ thống;

c) Các sự kiện xác thực;

d) Các sự kiện cấp, thu hồi quyền truy cập hệ thống và sử dụng dịch vụ;

đ) Xử lý giao dịch;

e) Các truy cập bất thường.

2. Ghi nhật ký giao dịch của khách hàng và giám sát các giao dịch tài chính trên hệ thống Internet Banking.

3. Các nhật ký của hệ thống Internet Banking phải được lưu trữ, bảo vệ an toàn và truy xuất được khi cần thiết. Thời gian lưu nhật ký tối thiểu là 03 năm.

4. Kiểm tra nhật ký truy cập để phát hiện, phòng ngừa những truy cập bất thường, bất hợp pháp tối thiểu mỗi tháng một lần.

Điều 12. Quản lý sự cố

1. Xây dựng quy trình quản lý sự cố, trong đó phải quy định rõ trách nhiệm của các bộ phận liên quan, chi tiết các bước thực hiện bao gồm cả việc thông báo cho khách hàng và báo cáo Ngân hàng Nhà nước.

2. Quy trình quản lý sự cố phải được rà soát, cập nhật các sự cố và phương án xử lý tối thiểu sáu tháng một lần.

3. Áp dụng các giải pháp kỹ thuật để phát hiện, xử lý kịp thời các cuộc tấn công từ chối dịch vụ như sử dụng thiết bị tường lửa; thiết bị phát hiện và ngăn chặn xâm

nhập; các thiết bị chuyên dụng cảnh báo tấn công, làm lệch hướng lưu lượng mạng; lọc gói tin khi bị tấn công.

4. Yêu cầu bên thứ ba cung cấp quy trình xử lý sự cố cho các dịch vụ do bên thứ ba cung cấp liên quan đến hệ thống Internet Banking.

Điều 13. Hướng dẫn khách hàng

1. Ban hành quy định nêu rõ quyền, nghĩa vụ của khách hàng và của đơn vị cung cấp dịch vụ đối với việc cung cấp, sử dụng dịch vụ Internet Banking.

2. Hướng dẫn cho khách hàng các nội dung tự bảo đảm an toàn trong quá trình sử dụng dịch vụ Internet Banking như:

a) Cách đặt mật khẩu và bảo vệ mật khẩu;

b) Không chia sẻ các thiết bị lưu trữ mật khẩu, chữ ký số;

c) Không đặt tùy chọn của trình duyệt web cho phép lưu lại tên và mật khẩu người dùng;

d) Thoát khỏi hệ thống Internet Banking khi không sử dụng;

đ) Thận trọng, hạn chế dùng máy tính công cộng, mạng không dây công cộng để truy cập vào hệ thống Internet Banking;

e) Cách thức truy cập địa chỉ ứng dụng dịch vụ Internet Banking của đơn vị;

g) Thông báo cho đơn vị cung cấp dịch vụ các lỗi và sự cố trong quá trình sử dụng dịch vụ;

h) Cảnh báo các rủi ro khác.

Chương III
BÁO CÁO

Điều 14. Yêu cầu chung

Các đơn vị cung cấp dịch vụ có trách nhiệm gửi báo cáo về Ngân hàng Nhà nước Việt Nam (Cục Công nghệ tin học) theo quy định tại Điều 15, Điều 16 Thông tư này.

Điều 15. Các loại báo cáo

1. Báo cáo cung cấp dịch vụ Internet Banking:

a) Đối với các đơn vị đã cung cấp dịch vụ trước ngày Thông tư này có hiệu lực: Các đơn vị gửi báo cáo trong vòng 10 ngày làm việc kể từ ngày Thông tư này có hiệu lực;

b) Đối với các đơn vị cung cấp dịch vụ sau khi Thông tư này có hiệu lực: Các đơn vị gửi báo cáo tối thiểu trước 10 ngày làm việc trước khi cung cấp chính thức dịch vụ Internet Banking.

2. Báo cáo năm:

Các đơn vị cung cấp dịch vụ phải gửi Báo cáo năm trước ngày 15 tháng 3 hàng năm.

3. Báo cáo đột xuất:

Các đơn vị cung cấp dịch vụ phải gửi Báo cáo đột xuất 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.

Điều 16. Nội dung báo cáo

1. Báo cáo cung cấp dịch vụ Internet Banking bao gồm các nội dung sau:

a) Địa chỉ website cung cấp dịch vụ;

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

c) Ngày cung cấp chính thức;

d) Đơn vị cung cấp sản phẩm hệ thống Internet Banking;

đ) 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;

e) Các tài liệu bao gồm: 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 vấn đề liên quan khác theo quy định tại Chương II của Thông tư này.

2. Báo cáo năm bao gồm các nội dung sau:

a) Các sản phẩm, dịch vụ Internet Banking hiện đang cung cấp;

b) Những thay đổi của sản phẩm, dịch vụ Internet Banking kể từ lần báo cáo trước;

c) Những thay đổi của tài liệu quy định tại Điểm e, Khoản 1, Điều 16 kể từ lần báo cáo trước;

d) Số lượng khách hàng sử dụng dịch vụ Internet Banking và tỷ lệ tăng trưởng khách hàng so với cùng kỳ năm trước;

đ) Những sự cố đã phát sinh trong kỳ. Sự cố rủi ro được báo cáo theo nhóm rủi ro, các thiệt hại và biện pháp xử lý đã áp dụng;

e) Kiến nghị, đề xuất.

3. Báo cáo đột xuất bao gồm các nội dung sau:

a) Ngày, địa điểm phát sinh sự cố;

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

c) Nguyên nhân sự cố;

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

đ) Tình hình thiệt hại;

e) Các biện pháp đơn vị đã tiến hành để khắc phục sự cố, ngăn chặn và phòng ngừa rủi ro;

g) Kiến nghị, đề xuất.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 17. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 04 tháng 11 năm 2011.

2. Thông tư số 09/2003/TT-NHNN ngày 05/8/2003 của Thống đốc Ngân hàng Nhà nước hướng dẫn thực hiện một số quy định tại Nghị định số 55/2001/NĐ-CP ngày 23/8/2001 của Chính phủ về quản lý, cung cấp và sử dụng Internet và Thông tư số 01/2008/TT-NHNN ngày 10/3/2008 sửa đổi bổ sung Thông tư số 09/2003/TT-NHNN hết hiệu lực kể từ ngày Thông tư này có hiệu lực thi hành.

3. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các tổ chức, cá nhân liên quan phản ánh kịp thời về Ngân hàng Nhà nước Việt Nam (Cục Công nghệ tin học tại địa chỉ số 64 Nguyễn Chí Thanh, Đống Đa, Hà Nội) để xem xét, xử lý.

Điều 18. Trách nhiệm thi hành

1. Cục Công nghệ tin học có trách nhiệm theo dõi, kiểm tra việc thi hành Thông tư này của các đơn vị cung cấp dịch vụ. Hàng năm thông qua báo cáo của các đơn vị hoặc thực hiện kiểm tra tại chỗ để đánh giá việc tuân thủ quy định và đảm bảo an toàn, bảo mật cho hệ thống Internet Banking của các đơn vị; tổng hợp, báo cáo Thống đốc tình hình về an toàn, bảo mật dịch vụ Internet Banking của hệ thống ngân hàng Việt Nam.

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.

3. 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 cung cấp dịch vụ Internet Banking chịu trách nhiệm thi hành Thông tư này./.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Nguyễn Toàn Thắng