NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
-------	Độc lập - Tự do - Hạnh phúc

Số: 01/2011/TT-NHNN	*Hà Nội, ngày 21 tháng 02 năm 2011*

THÔNG TƯ

QUY ĐỊNH VIỆC ĐẢM BẢO AN TOÀN, BẢO MẬT HỆ THỐNG CÔNG NGHỆ THÔNG TIN TRONG HOẠT ĐỘNG NGÂN HÀNG

Căn cứ Luật Ngân hàng Nhà nước Việt Nam số 46/2010/QH12 ngày 16/6/2010;
Căn cứ Luật các Tổ chức tín dụng số 47/2010/QH12 ngày 16/6/2010;
Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006;
Căn cứ Nghị định số 96/2008/NĐ-CP ngày 26/8/2008 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 việc đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng như sau:

Chương 1.

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 hệ thống công nghệ thông tin (CNTT) trong hoạt động ngân hàng.

2. Thông tư này áp dụng đối với Ngân hàng Nhà nước Việt Nam; các tổ chức tín dụng; chi nhánh ngân hàng nước ngoài (sau đây gọi chung là đơn vị).

Điều 2. Giải thích từ ngữ

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

1. *Hệ thống công nghệ thông tin:* là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của ngân hàng.

2. Tài sản CNTT: là các trang thiết bị, thông tin thuộc hệ thống CNTT của đơn vị. Bao gồm:

a) *Tài sản vật lý:* là các thiết bị CNTT, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống CNTT.

b) *Tài sản thông tin:* là các dữ liệu, tài liệu liên quan đến hệ thống CNTT. Tài sản thông tin được thể hiện bằng văn bản giấy hoặc dữ liệu điện tử.

c) *Tài sản phần mềm:* bao gồm các chương trình ứng dụng, phần mềm hệ thống, cơ sở dữ liệu và công cụ phát triển.

3. *Rủi ro CNTT:* là khả năng xảy ra tổn thất khi thực hiện các hoạt động liên quan đến hệ thống CNTT. Rủi ro CNTT liên quan đến quản lý, sử dụng phần cứng, phần mềm, truyền thông, giao diện hệ thống, vận hành và con người.

4. *Quản lý rủi ro:* là các hoạt động phối hợp nhằm xác định và kiểm soát các rủi ro CNTT có thể xảy ra.

5. *Bên thứ ba:* là các tổ chức, cá nhân có chuyên môn được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho hệ thống CNTT.

6. *Hệ thống an ninh mạng:* là tập hợp các thiết bị tường lửa; thiết bị kiểm soát, phát hiện truy cập bất hợp pháp; phần mềm quản trị, theo dõi, ghi nhật ký trạng thái an ninh mạng và các trang thiết bị khác có chức năng đảm bảo an toàn hoạt động của mạng, tất cả cùng hoạt động đồng bộ theo một chính sách an ninh mạng nhất quán nhằm kiểm soát chặt chẽ tất cả các hoạt động trên mạng.

7. *Tường lửa:* là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm được đặt giữa hai mạng, nhằm kiểm soát tất cả các kết nối từ bên trong ra bên ngoài mạng hoặc ngược lại.

8. *Vi rút:* là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số.

9. *Phần mềm độc hại (mã độc):* là các phần mềm có tính năng gây hại như vi rút, phần mềm do thám (spyware), phần mềm quảng cáo (adware) hoặc các dạng tương tự khác.

10. *Điểm yếu kỹ thuật:* là vị trí trong hệ thống CNTT dễ bị tổn thương khi bị tấn công hoặc xâm nhập bất hợp pháp.

Điều 3. Nguyên tắc chung

1. Từng đơn vị phải đảm bảo an toàn, bảo mật hệ thống CNTT của đơn vị mình theo các quy định tại Thông tư này.

2. Kịp thời nhận biết, phân loại, đánh giá và xử lý có hiệu quả các rủi ro CNTT có thể xảy ra trong đơn vị.

3. Xây dựng, triển khai quy chế an toàn, bảo mật hệ thống CNTT trên cơ sở hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của đơn vị.

4. Bố trí đủ nguồn lực có chất lượng phù hợp với quy mô nhằm đảm bảo an toàn, bảo mật hệ thống CNTT.

5. Xác định rõ quyền hạn, trách nhiệm của thủ trưởng đơn vị, các cấp, các bộ phận và từng cá nhân trong đơn vị đối với công tác đảm bảo an toàn, bảo mật hệ thống CNTT.

Điều 4. Quy chế an toàn, bảo mật hệ thống CNTT

1. Các đơn vị phải xây dựng quy chế an toàn, bảo mật hệ thống CNTT phù hợp với hệ thống CNTT, cơ cấu tổ chức, yêu cầu quản lý và hoạt động của đơn vị. Quy chế an toàn, bảo mật hệ thống CNTT phải được thủ trưởng đơn vị phê duyệt, tổ chức thực hiện và được triển khai tới tất cả các cán bộ, nhân viên và các bên liên quan.

2. Quy chế an toàn, bảo mật hệ thống CNTT phải bao gồm các quy định cơ bản về:

a) Quản lý tài sản CNTT;

b) Quản lý nguồn nhân lực;

c) Quy định về vật lý và môi trường;

d) Quy định về truyền thông và vận hành;

đ) Quản lý truy cập;

e) Tiếp nhận, phát triển, duy trì hệ thống thông tin;

g) Quản lý sự cố;

h) Lưu trữ và dự phòng thảm họa.

3. Định kỳ, đơn vị phải rà soát, chỉnh sửa, hoàn thiện quy chế an toàn, bảo mật hệ thống CNTT tối thiểu mỗi năm một lần, đảm bảo sự phù hợp, đầy đủ và có hiệu quả của quy chế. Trong trường hợp phát hiện những bất cập, bất hợp lý gây ra mất an toàn hệ thống CNTT hoặc theo yêu cầu của cơ quan có thẩm quyền, đơn vị phải tiến hành chỉnh sửa, bổ sung ngay quy chế của mình.

Chương 2.

CÁC QUY ĐỊNH VỀ ĐẢM BẢO AN TOÀN, BẢO MẬT HỆ THỐNG CÔNG NGHỆ THÔNG TIN

MỤC 1. TỔ CHỨC ĐẢM BẢO AN TOÀN, BẢO MẬT CNTT

Điều 5. Quản lý an toàn, bảo mật CNTT trong nội bộ đơn vị

1. Thủ trưởng đơn vị phải trực tiếp chỉ đạo công tác đảm bảo an toàn, bảo mật CNTT và quy định rõ trách nhiệm trong công tác đảm bảo an toàn, bảo mật CNTT cho các cá nhân, bộ phận.

2. Các cá nhân trong đơn vị liên quan đến bảo mật thông tin phải ký cam kết bảo mật thông tin.

Điều 6. Quản lý an toàn, bảo mật CNTT của đơn vị đối với bên thứ ba

1. Đánh giá về năng lực kỹ thuật, nhân sự, khả năng tài chính của bên thứ ba trước khi ký kết hợp đồng cung cấp hàng hóa, dịch vụ.

2. Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về an toàn, bảo mật CNTT khi ký hợp đồng. Hợp đồng với bên thứ ba phải bao gồm các điều khoản về việc xử phạt đối với bên thứ ba do vi phạm quy định an toàn, bảo mật thông tin và trách nhiệm phải bồi thường thiệt hại của bên thứ ba trong trường hợp có thiệt hại do hành vi vi phạm của bên thứ ba gây ra.

3. Đặc biệt chú ý đến các vấn đề về tính bí mật, tính toàn vẹn, tính sẵn sàng, tin cậy, hiệu năng tối đa, khả năng phục hồi thảm họa, phương tiện lưu trữ của hệ thống thông tin.

4. Xác định đầy đủ các rủi ro của đơn vị liên quan tới các bên thứ ba có thể phát sinh và áp dụng các biện pháp quản lý rủi ro.

5. Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép họ truy cập vào hệ thống CNTT của đơn vị.

MỤC 2. QUẢN LÝ TÀI SẢN CNTT

Điều 7. Xác định trách nhiệm đối với tài sản CNTT

1. Thống kê, kiểm kê các loại tài sản CNTT tại đơn vị mỗi năm tối thiểu một lần. Nội dung thống kê tài sản phải bao gồm các thông tin: Loại tài sản, giá trị, mức độ quan trọng, vị trí lắp đặt, thông tin dự phòng, thông tin về bản quyền.

2. Phân loại, sắp xếp thứ tự ưu tiên theo giá trị, mức độ quan trọng của tài sản CNTT để có biện pháp bảo vệ tài sản phù hợp. Xây dựng và thực hiện các quy định về quản lý, sử dụng tài sản.

3. Gắn quyền sử dụng tài sản cho các cá nhân hoặc bộ phận cụ thể. Người sử dụng tài sản CNTT phải tuân thủ các quy định về quản lý, sử dụng tài sản, đảm bảo tài sản được sử dụng đúng mục đích.

Điều 8. Phân loại tài sản thông tin

1. Phân loại tài sản thông tin theo các tiêu chí về giá trị, độ nhạy cảm và tầm quan trọng, tần suất sử dụng, thời gian lưu trữ.

2. Thực hiện các biện pháp quản lý phù hợp với từng loại tài sản thông tin đã phân loại.

MỤC 3. QUẢN LÝ NGUỒN NHÂN LỰC

Điều 9. Quản lý nguồn nhân lực nội bộ của đơn vị

1. Trước khi tuyển dụng hoặc phân công nhiệm vụ

a) Xác định trách nhiệm về an toàn, bảo mật CNTT của vị trí cần tuyển dụng hoặc phân công.

b) Kiểm tra lý lịch, xem xét đánh giá nghiêm ngặt tư cách đạo đức, trình độ chuyên môn khi tuyển dụng, phân công cán bộ, nhân viên làm việc tại các vị trí trọng yếu của hệ thống CNTT như quản trị hệ thống, quản trị hệ thống an ninh bảo mật, vận hành hệ thống, quản trị cơ sở dữ liệu.

c) Quyết định hoặc hợp đồng tuyển dụng (nếu có) phải bao gồm các điều khoản về trách nhiệm đảm bảo an toàn, bảo mật CNTT của người được tuyển dụng trong và sau khi làm việc tại đơn vị.

2. Trong thời gian làm việc

a) Đơn vị có trách nhiệm phổ biến và cập nhật các quy định về an toàn, bảo mật CNTT cho cán bộ, nhân viên.

b) Yêu cầu và kiểm tra việc thi hành các quy định về an toàn, bảo mật CNTT của cá nhân, tổ chức thuộc đơn vị tối thiểu mỗi năm một lần.

c) Áp dụng các biện pháp kỷ luật đối với cán bộ, nhân viên của đơn vị vi phạm quy định an toàn, bảo mật CNTT.

d) Những công việc quan trọng như cấu hình hệ thống an ninh mạng, thay đổi tham số hệ điều hành, cài đặt thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập (IPS) phải được thực hiện bởi ít nhất hai người hoặc phải có người giám sát.

đ) Không được cấp quyền quản trị (người có thể chỉnh sửa cấu hình, dữ liệu, nhật ký) trên hệ thống CNTT chính và hệ thống dự phòng cho cùng một cá nhân.

3. Khi chấm dứt hoặc thay đổi công việc

Khi cán bộ, nhân viên chấm dứt hoặc thay đổi công việc, đơn vị phải:

a) Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan về hệ thống CNTT.

b) Làm biên bản bàn giao tài sản với cán bộ, nhân viên.

c) Thu hồi hoặc thay đổi quyền truy cập hệ thống CNTT của cán bộ, nhân viên cho phù hợp với công việc được thay đổi.

Điều 10. Quản lý nguồn nhân lực bên thứ ba

1. Trước khi triển khai công việc

a) Yêu cầu bên thứ ba cung cấp danh sách nhân sự tham gia.

b) Kiểm tra tư cách pháp lý, năng lực chuyên môn của nhân sự bên thứ ba phù hợp với yêu cầu công việc.

c) Yêu cầu bên thứ ba ký cam kết không tiết lộ thông tin của đơn vị đối với các thông tin quan trọng.

2. Trong thời gian triển khai công việc

a) Cung cấp và yêu cầu bên thứ ba tuân thủ đầy đủ các quy chế, quy định về an toàn, bảo mật CNTT của đơn vị.

b) Giám sát việc tuân thủ các quy định an toàn, bảo mật CNTT của nhân sự bên thứ ba.

c) Trong trường hợp phát hiện dấu hiệu vi phạm hoặc vi phạm quy định an toàn, bảo mật thông tin của bên thứ ba, đơn vị cần:

- Tạm dừng hoặc đình chỉ hoạt động của bên thứ ba tùy theo mức độ vi phạm.

- Thông báo chính thức các vi phạm về an toàn, bảo mật CNTT của nhân sự cho bên thứ ba.

- Kiểm tra xác định, lập báo cáo mức độ vi phạm và thông báo cho bên thứ ba thiệt hại xảy ra.

- Thu hồi quyền truy cập hệ thống CNTT đã được cấp cho bên thứ ba.

3. Khi kết thúc công việc

a) Yêu cầu bên thứ ba bàn giao lại tài sản sử dụng của đơn vị trong quá trình triển khai công việc.

b) Thu hồi quyền truy cập hệ thống CNTT đã được cấp của bên thứ ba ngay sau khi kết thúc công việc.

c) Thay đổi các khóa, mật khẩu nhận bàn giao từ bên thứ ba.

MỤC 4. BẢO ĐẢM AN TOÀN VỀ MẶT VẬT LÝ VÀ MÔI TRƯỜNG

Điều 11. An toàn vật lý và môi trường

1. Các khu vực xử lý, lưu giữ thông tin và phương tiện xử lý thông tin phải được bảo vệ an toàn bằng tường bao, cổng ra vào có kiểm soát.

2. Các khu vực có yêu cầu cao về an toàn, bảo mật như phòng máy chủ phải áp dụng biện pháp kiểm soát ra vào thích hợp, đảm bảo chỉ những người có nhiệm vụ mới được vào khu vực đó.

3. Có biện pháp bảo vệ phòng chống nguy cơ do cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên và con người gây ra. Phòng máy chủ phải đảm bảo vệ sinh công nghiệp: Không dột, không thấm nước; các trang thiết bị lắp đặt trên sàn kỹ thuật, không bị ánh nắng chiếu rọi trực tiếp; độ ẩm, nhiệt độ đạt tiêu chuẩn quy định cho các thiết bị và máy chủ; trang bị đầy đủ thiết bị phòng chống cháy, nổ, lũ lụt, hệ thống chống sét.

4. Có nội quy, hướng dẫn làm việc trong khu vực an toàn, bảo mật.

5. Khu vực sử dụng chung, phân phối, chuyển hàng phải được kiểm soát và cách ly với khu vực an toàn, bảo mật.

Điều 12. An toàn, bảo mật tài sản CNTT

1. Tài sản CNTT phải được bố trí, lắp đặt tại các địa điểm an toàn và được bảo vệ để giảm thiểu những rủi ro do các đe dọa, hiểm họa từ môi trường và các xâm nhập trái phép.

2. Tài sản CNTT phải được bảo đảm về nguồn điện và các hệ thống hỗ trợ khi nguồn điện chính bị gián đoạn. Phải có biện pháp chống quá tải hay sụt giảm điện áp, chống sét lan truyền; có hệ thống tiếp giáp; có hệ thống máy phát điện dự phòng và hệ thống lưu điện đảm bảo thiết bị hoạt động liên tục.

3. Dây cáp cung cấp nguồn điện và dây cáp truyền thông sử dụng trong truyền tải dữ liệu hay những dịch vụ hỗ trợ thông tin phải được bảo vệ khỏi sự xâm phạm hoặc hư hại.

4. Tất cả các thiết bị lưu trữ dữ liệu phải được kiểm tra để đảm bảo các dữ liệu quan trọng và phần mềm có bản quyền lưu trữ trên thiết bị được xóa bỏ hoặc ghi đè không có khả năng khôi phục trước khi loại bỏ hoặc tái sử dụng cho mục đích khác.

5. Tài sản CNTT chỉ được đưa ra bên ngoài đơn vị khi có sự cho phép của cấp có thẩm quyền.

6. Các trang thiết bị dùng cho hoạt động nghiệp vụ lắp đặt bên ngoài trụ sở của đơn vị phải có biện pháp giám sát, bảo vệ an toàn phòng chống truy cập bất hợp pháp.

MỤC 5. QUẢN LÝ VẬN HÀNH VÀ TRUYỀN THÔNG

Điều 13. Quy trình vận hành

1. Ban hành và triển khai quy trình vận hành các hệ thống CNTT đến người sử dụng bao gồm: Quy trình bật, tắt thiết bị; quy trình sao lưu, phục hồi dữ liệu; quy trình bảo dưỡng thiết bị; quy trình vận hành ứng dụng; quy trình xử lý sự cố.

2. Kiểm soát sự thay đổi của hệ thống CNTT gồm: Phiên bản phần mềm, cấu hình phần cứng, tài liệu, quy trình vận hành; có phương án dự phòng cho việc phục hồi nếu sự thay đổi không thành

công hoặc gặp các sự cố không dự tính được; ghi chép lại các thay đổi; lập kế hoạch thực hiện và kiểm tra, thử nghiệm sự thay đổi trước khi áp dụng chính thức.

3. Hệ thống vận hành chính thức phải đáp ứng yêu cầu:

- Tách biệt với môi trường phát triển và môi trường kiểm tra, thử nghiệm.

- Chỉ cho phép kết nối Internet đối với hệ thống CNTT đã được áp dụng đầy đủ các giải pháp an ninh, an toàn và đủ khả năng bảo vệ trước các hiểm họa, tấn công từ bên ngoài.

- Không cài đặt các công cụ, phương tiện phát triển ứng dụng trên hệ thống vận hành chính thức.

4. Đối với hệ thống thông tin nghiệp vụ:

a) Không để một cá nhân làm toàn bộ các khâu từ khởi tạo đến phê duyệt một giao dịch nghiệp vụ.

b) Mọi tác vụ trên hệ thống được lưu vết, sẵn sàng cho kiểm tra, kiểm soát khi cần thiết.

Điều 14. Quản lý các dịch vụ do bên thứ ba cung cấp

1. Phải giám sát và kiểm tra các dịch vụ do bên thứ ba cung cấp đảm bảo mức độ cung cấp dịch vụ, khả năng hoạt động hệ thống đáp ứng đúng theo thỏa thuận đã ký kết.

2. Đảm bảo triển khai, duy trì các biện pháp an toàn, bảo mật của dịch vụ do bên thứ ba cung cấp theo đúng thỏa thuận.

3. Quản lý các thay đổi đối với các dịch vụ của bên thứ ba cung cấp bao gồm: Nâng cấp phiên bản mới; sử dụng các kỹ thuật mới, các công cụ và môi trường phát triển mới. Đánh giá đầy đủ tác động của việc thay đổi, đảm bảo an toàn khi được đưa vào sử dụng.

Điều 15. Quản lý việc lập kế hoạch và chấp nhận hệ thống CNTT

1. Giám sát và tối ưu hiệu suất của hệ thống CNTT; lập kế hoạch về hiệu suất, dung lượng của hệ thống CNTT trong tương lai nhằm đảm bảo tiêu chuẩn cần thiết.

2. Xây dựng các yêu cầu, tiêu chuẩn như hiệu năng, thời gian phục hồi khi gặp sự cố, đảm bảo tính liên tục; đào tạo và chuyển giao kỹ thuật đối với những nội dung thay đổi cho người sử dụng và thực hiện kiểm tra đánh giá khả năng đáp ứng của hệ thống CNTT mới hoặc hệ thống nâng cấp trước khi áp dụng chính thức.

Điều 16. Sao lưu dự phòng

1. Ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết.

2. Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

3. Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu sáu tháng một lần.

Điều 17. Quản lý về an toàn, bảo mật mạng

1. Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các hiểm họa và duy trì an toàn cho các hệ thống, ứng dụng sử dụng mạng:

a) Có sơ đồ logic và vật lý về hệ thống mạng;

b) Sử dụng thiết bị tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập và các trang thiết bị khác đảm bảo an toàn bảo mật mạng.

2. Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an ninh mạng. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

3. Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ mạng do bên thứ ba cung cấp.

Điều 18. Trao đổi thông tin

1. Ban hành các quy định trao đổi thông tin và phần mềm qua mạng truyền thông trong đơn vị và với các đơn vị khác. Xác định trách nhiệm và nghĩa vụ pháp lý với các thành phần tham gia.

2. Có thỏa thuận cho việc trao đổi thông tin với bên ngoài.

3. Có biện pháp bảo vệ phương tiện mang tin khi vận chuyển.

4. Xây dựng và thực hiện các biện pháp bảo vệ thông tin trao đổi giữa các hệ thống CNTT.

Điều 19. Các dịch vụ thương mại điện tử

1. Có biện pháp bảo vệ thông tin trong thương mại điện tử nhằm chống lại các hoạt động gian lận, sửa đổi trái phép:

a) Đường truyền và giao thức truyền thông phải được mã hóa;

b) Sử dụng các phương thức xác thực mạnh như xác thực đa thành phần hoặc chữ ký số cho các thành viên tham gia giao dịch.

2. Thông tin trong các giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép.

3. Thông tin công khai trên các hệ thống CNTT phải được bảo vệ nhằm ngăn chặn sự sửa đổi trái phép.

Điều 20. Giám sát và ghi nhật ký hoạt động của hệ thống CNTT

1. Ghi nhật ký và quy định thời gian lưu trữ các thông tin về hoạt động của hệ thống CNTT và người sử dụng, lỗi phát sinh và các sự cố mất an toàn thông tin nhằm trợ giúp cho việc điều tra giám sát về sau.

2. Xem xét và lập báo cáo định kỳ về nhật ký và có các hoạt động xử lý các lỗi, sự cố cần thiết.

3. Bảo vệ các chức năng ghi nhật ký và thông tin nhật ký, chống giả mạo và truy cập trái phép. Người quản trị hệ thống và người sử dụng không được xóa hay sửa đổi nhật ký hệ thống ghi lại các hoạt động của chính họ.

4. Có cơ chế đồng bộ thời gian giữa các hệ thống CNTT.

Điều 21. Phòng chống vi rút và phần mềm độc hại

Xây dựng và thực hiện quy định về phòng chống vi rút, mã độc đáp ứng các yêu cầu cơ bản sau:

1. Triển khai hệ thống phòng chống vi rút máy tính cho toàn bộ hệ thống CNTT của đơn vị.

2. Kiểm tra, diệt vi rút, mã độc cho toàn bộ hệ thống CNTT của đơn vị hàng ngày và phương tiện mang tin nhận từ bên ngoài trước khi sử dụng.

3. Không mở các thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ để tránh vi rút, mã độc.

4. Không vào các trang web không có nguồn gốc xuất xứ rõ ràng, đáng ngờ.

5. Cập nhật kịp thời các mẫu vi rút, mã độc mới và các phần mềm chống vi rút, mã độc mới.

6. Báo ngay cho người quản trị hệ thống xử lý trong trường hợp phát hiện nhưng không diệt được vi rút, mã độc.

7. Không tự ý cài đặt các phần mềm khi chưa được phép của người quản trị hệ thống.

MỤC 6. CÁC BIỆN PHÁP QUẢN LÝ TRUY CẬP

Điều 22. Yêu cầu nghiệp vụ đối với kiểm soát truy cập

1. Xây dựng và thực hiện các quy định về quản lý truy cập đối với người sử dụng, nhóm người sử dụng, đảm bảo đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn, bảo mật. Quy định về quản lý truy cập bao gồm các nội dung cơ bản sau:

a) Đăng ký, cấp phát, gia hạn và thu hồi quyền truy cập của người sử dụng;

b) Giới hạn và kiểm soát các truy cập đặc quyền;

c) Quản lý, cấp phát mật khẩu;

d) Rà soát, kiểm tra, xét duyệt lại quyền truy cập của người sử dụng.

2. Quy định về quản lý mật khẩu phải đáp ứng các yêu cầu sau:

a) Mật khẩu phải có độ dài sáu ký tự trở lên, cấu tạo gồm các ký tự số, chữ và các ký tự đặc biệt khác nếu hệ thống cho phép. Các yêu cầu mật khẩu hợp lệ phải được kiểm tra tự động khi thiết lập mật khẩu;

b) Các mật khẩu mặc định của nhà sản xuất cài đặt sẵn trên các trang thiết bị, phần mềm, cơ sở dữ liệu phải được thay đổi ngay khi đưa vào sử dụng;

c) Phần mềm quản lý mật khẩu phải có các chức năng: Thông báo người sử dụng thay đổi mật khẩu sắp hết hạn sử dụng; hủy hiệu lực của mật khẩu hết hạn sử dụng; cho phép thay đổi ngay mật khẩu bị lộ, có nguy cơ bị lộ hoặc theo yêu cầu của người sử dụng; ngăn chặn việc sử dụng lại mật khẩu cũ trong một khoảng thời gian nhất định.

3. Quy định trách nhiệm người sử dụng khi được cấp quyền truy cập: Sử dụng mật khẩu đúng quy định, giữ bí mật mật khẩu, thoát khỏi hệ thống khi không làm việc trên hệ thống hoặc tạm thời không làm việc trên hệ thống.

Điều 23. Quản lý truy cập mạng

1. Ban hành các quy định sử dụng mạng và các dịch vụ mạng; các thủ tục cấp phép, xóa bỏ quyền kết nối đến mạng và dịch vụ mạng; những cách thức, phương tiện truy cập mạng, dịch vụ mạng. Trong đó quy định rõ:

a) Các mạng và dịch vụ mạng được phép sử dụng;

b) Các điều kiện để được kết nối mạng.

2. Sử dụng các biện pháp thích hợp để xác thực người sử dụng kết nối từ bên ngoài vào mạng nội bộ của đơn vị đảm bảo an toàn, bảo mật.

3. Kiểm soát truy cập các cổng dùng để cấu hình và quản trị thiết bị mạng.

4. Chia tách hệ thống mạng thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng và hệ thống thông tin.

Điều 24. Kiểm soát truy cập hệ điều hành

1. Có quy trình để kiểm soát truy cập hệ điều hành; quy định quản lý mật khẩu truy cập hệ điều hành an toàn, bảo mật.

2. Mỗi người sử dụng hệ điều hành phải có một định danh duy nhất và được xác thực, nhận dạng, lưu dấu vết khi truy cập hệ điều hành.

3. Sử dụng thêm các phương pháp xác thực khác như sinh trắc học hoặc thẻ đối với các máy chủ quan trọng ngoài việc xác thực bằng mật khẩu.

4. Quy định giới hạn và kiểm soát chặt chẽ những tiện ích hệ thống có khả năng ảnh hưởng đến hệ thống và chương trình ứng dụng khác.

5. Tự động ngắt phiên làm việc sau một thời gian không sử dụng, nhằm ngăn chặn sự truy cập trái phép.

6. Quy định giới hạn thời gian kết nối với những ứng dụng có độ rủi ro cao.

Điều 25. Kiểm soát truy cập thông tin và ứng dụng

1. Quản lý và phân quyền truy cập thông tin và ứng dụng phù hợp với chức năng nhiệm vụ của người sử dụng:

a) Phân quyền truy cập đến từng thư mục, chức năng của chương trình;

b) Phân quyền đọc, ghi, xóa, thực thi đối với thông tin, dữ liệu, chương trình.

2. Các hệ thống thông tin quan trọng phải đặt trong môi trường mạng máy tính riêng. Nếu các hệ thống thông tin cùng sử dụng nguồn tài nguyên chung thì phải được người quản trị hệ thống chấp nhận.

MỤC 7. TIẾP NHẬN, PHÁT TRIỂN, DUY TRÌ HỆ THỐNG THÔNG TIN

Điều 26. Yêu cầu về an toàn, bảo mật cho các hệ thống thông tin

Khi xây dựng hệ thống thông tin mới hoặc cải tiến hệ thống thông tin hiện tại, phải đưa ra các yêu cầu về an toàn, bảo mật đồng thời với việc đưa ra các yêu cầu kỹ thuật, nghiệp vụ.

Điều 27. Đảm bảo an toàn, bảo mật các ứng dụng

Các chương trình ứng dụng nghiệp vụ phải đạt được các yêu cầu sau:

1. Kiểm tra tính hợp lệ của dữ liệu nhập vào các ứng dụng, đảm bảo dữ liệu được nhập vào chính xác và hợp lệ.

2. Kiểm tra tính hợp lệ của dữ liệu cần được xử lý tự động trong các ứng dụng nhằm phát hiện thông tin sai lệch do các lỗi trong quá trình xử lý hoặc các hành vi sửa đổi thông tin có chủ ý.

3. Có các biện pháp đảm bảo tính xác thực và bảo vệ sự toàn vẹn của dữ liệu được xử lý trong các ứng dụng.

4. Kiểm tra tính hợp lệ của dữ liệu xuất ra từ các ứng dụng, đảm bảo quá trình xử lý thông tin của các ứng dụng là chính xác và hợp lệ.

Điều 28. Quản lý mã hóa

1. Quy định và đưa vào sử dụng các biện pháp mã hóa và quản lý khóa theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin của đơn vị. Sử dụng các giải thuật mã hóa như:

a) AES: Advanced Encryption Standard;

b) 3DES: Triple Data Encryption Standard;

c) RSA: Rivest-Shamir-Adleman;

d) Giải thuật khác.

2. Dữ liệu về mật khẩu khách hàng, mật khẩu người sử dụng và các dữ liệu nhạy cảm khác phải được mã hóa khi truyền lên mạng và khi lưu trữ.

Điều 29. An toàn, bảo mật các tệp tin hệ thống

1. Quy định về quản lý, cài đặt, cập nhật các phần mềm lên hệ thống hiện tại, đảm bảo an toàn cho các tệp tin hệ thống.

2. Dữ liệu kiểm tra, thử nghiệm phải được lựa chọn, bảo vệ, quản lý và kiểm soát một cách thận trọng.

3. Việc truy cập vào chương trình nguồn phải được quản lý và kiểm soát chặt chẽ.

Điều 30. An toàn, bảo mật trong quy trình hỗ trợ và phát triển

1. Phải có quy định về quản lý và kiểm soát sự thay đổi hệ thống thông tin.

2. Khi thay đổi hệ điều hành phải kiểm tra và xem xét các ứng dụng nghiệp vụ quan trọng để đảm bảo hệ thống hoạt động ổn định, an toàn trên môi trường mới.

3. Việc sửa đổi các gói phần mềm phải được quản lý và kiểm soát chặt chẽ.

4. Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài.

Điều 31. Quản lý các điểm yếu về mặt kỹ thuật

1. Có quy định về việc đánh giá, quản lý và kiểm soát các điểm yếu kỹ thuật của các hệ thống CNTT đang sử dụng. Định kỳ đánh giá, lập báo cáo về các điểm yếu kỹ thuật của các hệ thống CNTT đang sử dụng.

2. Xây dựng và triển khai các giải pháp khắc phục các điểm yếu kỹ thuật, hạn chế các rủi ro liên quan.

MỤC 8. QUẢN LÝ CÁC SỰ CỐ VỀ CNTT

Điều 32. Báo cáo sự cố

1. Xây dựng quy trình báo cáo, các mẫu báo cáo và xác định rõ người nhận báo cáo về các sự cố CNTT.

2. Quy định rõ trách nhiệm báo cáo của cán bộ, nhân viên và bên thứ ba về các sự cố CNTT.

3. Các sự cố mất an toàn phải được lập tức báo cáo đến những người có thẩm quyền và những người có liên quan để có biện pháp khắc phục trong thời gian sớm nhất.

Điều 33. Kiểm soát và khắc phục sự cố

1. Ban hành quy trình, trách nhiệm khắc phục và phòng ngừa sự cố CNTT, đảm bảo sự cố được xử lý trong thời gian ngắn nhất và giảm thiểu khả năng sự cố lặp lại.

2. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị.

3. Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố về CNTT có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

MỤC 9. ĐẢM BẢO HOẠT ĐỘNG LIÊN TỤC CỦA CÁC HỆ THỐNG CNTT

Điều 34. Đảm bảo hoạt động liên tục

1. Căn cứ quy mô và mức độ quan trọng của từng hệ thống CNTT đối với hoạt động của đơn vị để lựa chọn ra các hệ thống CNTT trọng yếu, có ảnh hưởng lớn tới hoạt động của đơn vị.

2. Xây dựng và triển khai kế hoạch, quy trình đảm bảo hoạt động liên tục của các hệ thống CNTT trọng yếu.

3. Tối thiểu sáu tháng một lần, tiến hành kiểm tra, thử nghiệm, đánh giá và cập nhật các quy trình đảm bảo hoạt động liên tục của các hệ thống CNTT trọng yếu.

4. Kế hoạch, quy trình đảm bảo hoạt động liên tục phải được kiểm tra, đánh giá và cập nhật khi có sự thay đổi của hệ thống.

Điều 35. Công tác dự phòng thảm họa

1. Xây dựng hệ thống dự phòng cho các hệ thống CNTT trọng yếu của đơn vị. Các hệ thống dự phòng cách hệ thống chính tối thiểu 30 km tính theo đường thẳng nối giữa hai hệ thống.

2. Hệ thống dự phòng phải thay thế được hệ thống chính trong vòng 4 giờ kể từ khi hệ thống chính có sự cố không khắc phục được.

3. Tối thiểu ba tháng một lần, phải chuyển hoạt động từ hệ thống chính sang hệ thống dự phòng để đảm bảo tính đồng nhất và sẵn sàng của hệ thống dự phòng.

4. Tối thiểu ba tháng một lần, tiến hành kiểm tra, đánh giá hoạt động của hệ thống dự phòng.

MỤC 10. KIỂM TRA NỘI BỘ VÀ BÁO CÁO

Điều 36. Kiểm tra nội bộ

1. Các đơn vị phải tự tổ chức kiểm tra việc tuân thủ các quy định tại Thông tư này tối thiểu mỗi năm một lần.

2. Kết quả kiểm tra và các kiến nghị đề xuất phải được lập thành báo cáo.

Điều 37. Báo cáo

Các đơn vị có trách nhiệm gửi báo cáo về Ngân hàng Nhà nước Việt Nam (Cục Công nghệ tin học) như sau:

1. Quy chế an toàn, bảo mật CNTT của đơn vị:

a) Đối với các đơn vị đã ban hành quy chế an toàn, bảo mật CNTT trước ngày Thông tư này có hiệu lực: Các đơn vị gửi quy chế an toàn, bảo mật CNTT trong thời hạn 15 ngày kể từ ngày Thông tư này có hiệu lực.

b) Đối với các đơn vị chưa ban hành quy chế an toàn, bảo mật CNTT kể từ ngày Thông tư này có hiệu lực: Các đơn vị phải ban hành và gửi quy chế an toàn, bảo mật CNTT trong thời hạn 6 tháng kể từ ngày Thông tư này có hiệu lực.

2. Báo cáo năm:

a) Các chỉnh sửa, bổ sung quy chế an toàn, bảo mật CNTT nếu có; Báo cáo kiểm tra nội bộ của đơn vị theo quy định tại Điều 36 của Thông tư này.

b) Thời hạn gửi báo cáo: Trước ngày 15 tháng 3 hàng năm.

c) Hình thức và mẫu báo cáo: Theo hướng dẫn của Ngân hàng Nhà nước Việt Nam (Cục Công nghệ tin học).

3. Báo cáo đột xuất:

Khi xảy ra các vụ, việc mất an toàn đối với hệ thống CNTT, đơn vị gửi báo cáo đột xuất bằng văn bản, cụ thể như sau:

a) Thời hạn gửi báo cáo: Trong thời hạn 10 ngày kể từ thời điểm vụ, việc được phát hiện.

b) Nội dung báo cáo đột xuất:

- Ngày, địa điểm phát sinh vụ, việc;

- Nguyên nhân vụ, việc;

- Đánh giá rủi ro, ảnh hưởng đối với hệ thống CNTT và nghiệp vụ tại nơi xảy ra vụ, việc và những địa điểm khác có liên quan;

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

- Kiến nghị, đề xuất.

Chương 3.

ĐIỀU KHOẢN THI HÀNH

Điều 38. Xử lý vi phạm

Các tổ chức, cá nhân vi phạm quy định tại Thông tư này, tùy theo mức độ vi phạm sẽ bị xử lý theo các quy định của pháp luật.

Điều 39. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành sau bốn mươi lăm ngày kể từ ngày ký ban hành và thay thế các văn bản sau:

- Quyết định số 04/2006/QĐ-NHNN ngày 18/01/2006 của Thống đốc Ngân hàng Nhà nước ban hành Quy chế an toàn, bảo mật hệ thống công nghệ thông tin trong ngành Ngân hàng;

- Quyết định số 14/2000/QĐ-NHNN16 ngày 07/01/2000 của Thống đốc Ngân hàng Nhà nước về việc ban hành Quy chế quản lý, sử dụng hệ thống tin học trong ngành Ngân hàng;

- Quyết định số 864/2003/QĐ-NHNN ngày 05/8/2003 của Thống đốc Ngân hàng Nhà nước về việc sửa đổi, bổ sung một số điều của Quy chế quản lý, sử dụng hệ thống tin học trong ngành Ngân hàng ban hành kèm theo Quyết định số 14/2000/QĐ-NHNN16 ngày 07/01/2000.

2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Ngân hàng Nhà nước Việt Nam để xem xét, bổ sung, sửa đổi.

Điều 40. 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.

2. Cơ quan Thanh tra, giám sát ngân hàng có trách nhiệm phối hợp với Cục Công nghệ tin học kiểm tra việc thi hành Thông tư này đối với các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài và xử lý vi phạm hành chính đối với hành vi vi phạm theo quy định của pháp luật.

3. Vụ Kiểm toán nội bộ có trách nhiệm thực hiện kiểm toán nội bộ việc thi hành Thông tư này đối với các đơn vị thuộc Ngân hàng Nhà nước Việt Nam.

4. Thủ trưởng các đơn vị liên quan 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, Tổng giám đốc (Giám đốc) các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài có trách nhiệm tổ chức triển khai và kiểm tra việc thi hành tại đơn vị mình theo đúng các quy định của Thông tư này.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Nơi nhận:
- Như Khoản 4 Điều 40;
- Ban lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Lưu: VP, CNTH, PC.

Nguyễn Toàn Thắng