NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 31 /2015/TT-NHNN	*Hà Nội, ngày 28 tháng 12 năm 2015*

THÔNG TƯ
Quy định về 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 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 Công nghệ thông tin số 67/2006/QH11 ngày 29 tháng 6 năm 2006;

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

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 đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng.

Chương I
QUY ĐỊNH CHUNG

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

1. Thông tư này quy định về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng.

2. Thông tư này áp dụng đối với Ngân hàng Nhà nước Việt Nam (Ngân hàng Nhà nước), các tổ chức tín dụng (trừ quỹ tín dụng nhân dân cơ sở có tài sản dưới 10 tỷ, tổ chức tài chính vi mô), chi nhánh ngân hàng nước ngoài, các tổ chức cung ứng

dịch vụ trung gian thanh toán (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 để sản xuất, truyền nhận, thu thập, xử lý, lưu trữ và trao đổi thông tin số phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của đơn vị.

2. Hệ thống công nghệ thông tin quan trọng là hệ thống công nghệ thông tin khi phát sinh sự cố sẽ làm tổn hại nghiêm trọng đến hoạt động của đơn vị hoặc làm tổn hại tới lợi ích của khách hàng đang sử dụng dịch vụ của đơn vị.

3. Trung tâm dữ liệu bao gồm hạ tầng kỹ thuật (nhà trạm, hệ thống cáp) và hệ thống máy tính cùng các thiết bị phụ trợ được lắp đặt vào đó để lưu trữ, trao đổi và quản lý tập trung dữ liệu của một hay nhiều tổ chức, cá nhân.

4. Thiết bị di động là thiết bị số có thể cầm tay, có hệ điều hành, có khả năng xử lý, kết nối mạng và có màn hình hiển thị như máy tính xách tay, máy tính bảng, điện thoại di động thông minh.

5. Vật mang tin là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin điện tử.

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

7. Quản lý rủi ro công nghệ thông tin là các hoạt động phối hợp nhằm nhận diện và kiểm soát các rủi ro công nghệ thông tin có thể xảy ra.

8. Dữ liệu nhạy cảm là dữ liệu có thông tin mật, thông tin lưu hành nội bộ của đơn vị hoặc do đơn vị quản lý, nếu lộ lọt ra ngoài sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của đơn vị.

9. Tài khoản người dùng là một tập hợp thông tin đại diện duy nhất cho người sử dụng trên hệ thống công nghệ thông tin, người dùng sử dụng để đăng nhập và truy cập các tài nguyên được cấp phép trên hệ thống công nghệ thông tin đó. Tài khoản người dùng ít nhất phải bao gồm tên định danh và mã khóa bí mật.

10. Bên thứ ba là các tổ chức, cá nhân được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hoá, dịch vụ kỹ thuật cho hệ thống công nghệ thông tin.

11. 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.

12. Phần mềm độc hại (mã độc) là phần mềm có khả năng gây ra hoạt động

không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

13. Điểm yếu về mặt kỹ thuật là vị trí trong hệ thống công nghệ thông tin dễ bị khai thác, lợi dụng khi bị tấn công hoặc xâm nhập bất hợp pháp.

14. Tính bảo mật của thông tin là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng.

15. Tính toàn vẹn của thông tin là bảo vệ sự chính xác và đầy đủ của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền.

16. Tính sẵn sàng của thông tin là đảm bảo những người được cấp quyền có thể truy xuất thông tin ngay khi có nhu cầu.

17. An ninh mạng là sự bảo vệ hệ thống công nghệ thông tin và thông tin truyền đưa trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính toàn vẹn, tính bảo mật và tính sẵn sàng của thông tin.

Điều 3. Nguyên tắc chung

1. Từng đơn vị phải đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin của đơn vị mình.

2. Xác định các hệ thống công nghệ thông tin quan trọng và áp dụng chính sách đảm bảo an toàn bảo mật phù hợp.

3. Nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả các rủi ro công nghệ thông tin có thể xảy ra trong đơn vị.

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

5. Bố trí nhân sự chuyên trách chịu trách nhiệm đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin.

6. Xác định rõ quyền hạn, trách nhiệm của thủ trưởng đơn vị (hoặc người đại diện hợp pháp), từng bộ phận và cá nhân trong đơn vị đối với công tác đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin.

Điều 4. Quy chế an toàn, bảo mật hệ thống công nghệ thông tin

1. Các đơn vị phải xây dựng quy chế an toàn, bảo mật hệ thống công nghệ thông tin phù hợp với hệ thống công nghệ thông tin, cơ cấu tổ chức, yêu cầu quản lý và hoạt động của đơn vị. Quy chế an toàn, bảo mật hệ thống công nghệ thông tin phải được thủ trưởng đơn vị (hoặc người đại diện hợp pháp) ký ban hành, tổ chức thực hiện, triển khai trong toàn đơn vị.

2. Quy chế an toàn, bảo mật hệ thống công nghệ thông tin quy định về các nội dung cơ bản sau:

a) Quản lý tài sản công nghệ thông tin; quản lý sử dụng thiết bị di động; quản

lý sử dụng vật mang tin;

b) Quản lý nguồn nhân lực;

c) Đảm bảo an toàn về mặt vật lý và môi trường;

d) Quản lý vận hành và truyền thông;

đ) Quản lý truy cập;

e) Quản lý dịch vụ công nghệ thông tin của bên thứ ba;

g) Quản lý tiếp nhận, phát triển, duy trì hệ thống thông tin;

h) Quản lý sự cố công nghệ thông tin;

i) Đảm bảo hoạt động liên tục của hệ thống công nghệ thông tin;

k) Kiểm tra, báo cáo hoạt động công nghệ thông tin.

3. Đơn vị phải rà soát, chỉnh sửa, hoàn thiện quy chế an toàn, bảo mật hệ thống công nghệ thông tin tối thiểu mỗi năm một lần, đảm bảo sự đầy đủ của quy chế theo các quy định tại Thông tư này. Khi phát hiện những bất cập, bất hợp lý gây ra mất an toàn hệ thống công nghệ thông tin hoặc theo yêu cầu của cơ quan có thẩm quyền, đơn vị phải tiến hành chỉnh sửa, bổ sung ngay quy chế an toàn, bảo mật hệ thống công nghệ thông tin đã ban hành.

Chương II

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

Mục 1

QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

Điều 5. Quản lý tài sản công nghệ thông tin

1. Các loại tài sản công nghệ thông tin bao gồm:

a) Tài sản vật lý: các thiết bị công nghệ thông tin, phương tiện truyền thông và các thiết bị phục vụ cho hoạt động của hệ thống công nghệ thông tin;

b) Tài sản thông tin: các dữ liệu, thông tin ở dạng số, tài liệu được thể hiện bằng văn bản giấy hoặc các phương tiện khác;

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

2. Đơn vị thực hiện việc lập danh sách của tất cả các tài sản công nghệ thông tin, rà soát và cập nhật danh sách này tối thiểu một năm một lần.

3. Căn cứ phân loại tài sản công nghệ thông tin tại Khoản 1 Điều này, đơn vị

xây dựng và thực hiện các quy định về quản lý và sử dụng tài sản theo quy định tại Điều 6, 7, 8, 9 và Điều 10 Thông tư này.

Điều 6. Quản lý tài sản vật lý

1. Danh sách tài sản vật lý được lập với các thông tin cơ bản gồm: tên tài sản, giá trị, mức độ quan trọng, vị trí lắp đặt, mục đích sử dụng, tình trạng sử dụng, thông tin về bản quyền (nếu có).

2. Đơn vị phải xác định, đánh giá mức độ rủi ro, mức độ quan trọng, yêu cầu về tính sẵn sàng của tài sản vật lý để phân loại, sắp xếp tài sản và thực hiện việc trang bị, biện pháp bảo vệ phù hợp. Đối với tài sản vật lý là cấu phần của hệ thống công nghệ thông tin quan trọng tại trung tâm dữ liệu chính phải có biện pháp dự phòng đảm bảo tính sẵn sàng cao cho hoạt động liên tục.

3. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng.

4. Tài sản vật lý khi mang ra khỏi đơn vị phải được sự phê duyệt của thủ trưởng đơn vị hoặc người được thủ trưởng ủy quyền. Đối với tài sản vật lý có chứa thông tin, dữ liệu nhạy cảm trước khi mang ra khỏi đơn vị phải thực hiện biện pháp bảo vệ để giữ bí mật đối với thông tin, dữ liệu lưu trữ trên tài sản đó.

5. Đơn vị phải xây dựng kế hoạch, quy trình bảo trì, bảo dưỡng và tổ chức thực hiện đối với từng chủng loại tài sản vật lý theo quy định của Ngân hàng Nhà nước về bảo trì trang thiết bị tin học trong ngành ngân hàng.

6. Tài sản vật lý có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện biện pháp tiêu hủy cấu phần lưu trữ dữ liệu trên tài sản đó.

7. Đối với tài sản vật lý là thiết bị di động, vật mang tin, ngoài các quy định tại Điều này, đơn vị xây dựng và thực hiện quản lý theo quy định tại Điều 9, Điều 10 Thông tư này.

Điều 7. Quản lý tài sản thông tin

1. Đơn vị phải lập danh mục, quy định về thẩm quyền, trách nhiệm của người được tiếp cận, khai thác đối với các loại tài sản thông tin.

2. Đơn vị phải phân loại và đánh giá mức độ rủi ro, tầm quan trọng dựa trên yêu cầu về tính bảo mật, tính toàn vẹn, tính sẵn sàng cho việc sử dụng của tài sản thông tin để thực hiện các biện pháp quản lý, bảo vệ phù hợp.

3. Đối với tài sản thông tin chứa dữ liệu nhạy cảm, đơn vị phải thực hiện các biện pháp mã hóa để đảm bảo an toàn, bảo mật trong quá trình trao đổi, lưu trữ.

Điều 8. Quản lý tài sản phần mềm

1. Danh sách tài sản phần mềm được lập với các thông tin cơ bản gồm: tên tài

sản, giá trị, mức độ quan trọng, mục đích sử dụng, phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, nơi lưu giữ.

2. Đơn vị phải phân loại và đánh giá mức độ rủi ro dựa trên yêu cầu về tính bảo mật, tính toàn vẹn, tính sẵn sàng cho việc sử dụng của tài sản phần mềm để thực hiện các biện pháp quản lý, bảo vệ phù hợp.

3. Đơn vị phải xây dựng kế hoạch, quy trình bảo trì và tổ chức thực hiện đối với từng loại tài sản phần mềm theo quy định của Ngân hàng Nhà nước về bảo trì trang thiết bị tin học trong ngành ngân hàng.

Điều 9. Quản lý sử dụng thiết bị di động

1. Các thiết bị di động khi kết nối vào hệ thống mạng nội bộ của đơn vị phải được đăng ký để kiểm soát.

2. Giới hạn phạm vi kết nối từ thiết bị di động đến các dịch vụ, hệ thống thông tin của đơn vị; kiểm soát các kết nối từ thiết bị di động tới các hệ thống thông tin được phép sử dụng tại đơn vị.

3. Đơn vị phải quy định trách nhiệm của người sử dụng thiết bị di động, bao gồm các yêu cầu tối thiểu sau:

a) Bảo vệ thiết bị chống hư hỏng, mất cắp, thất lạc;

b) Kiểm soát các phần mềm được cài đặt; cập nhật các phiên bản phần mềm và các bản vá lỗi trên thiết bị di động;

c) Cài đặt tính năng mã hóa dữ liệu; mã khóa bí mật bảo vệ; phần mềm phòng chống mã độc và các lỗi bảo mật khác;

d) Thiết lập chức năng vô hiệu hóa, khóa thiết bị hoặc xóa dữ liệu từ xa trong trường hợp thất lạc hoặc bị mất cắp;

đ) Sao lưu dữ liệu trên thiết bị di động nhằm bảo vệ, khôi phục dữ liệu khi cần thiết;

e) Thực hiện các biện pháp bảo vệ dữ liệu khi bảo hành, bảo trì, sửa chữa thiết bị di động.

Điều 10. Quản lý sử dụng vật mang tin

Đơn vị có trách nhiệm:

1. Kiểm soát việc đấu nối, gỡ bỏ vật mang tin với thiết bị thuộc hệ thống công nghệ thông tin.

2. Triển khai các biện pháp bảo đảm an toàn vật mang tin khi vận chuyển, lưu trữ.

3. Thực hiện biện pháp bảo vệ đối với dữ liệu nhạy cảm chứa trong vật mang tin.

4. Khi không sử dụng được hoặc sử dụng vật mang tin chứa dữ liệu nhạy cảm

cho mục đích khác phải thực hiện xóa, tiêu hủy dữ liệu lưu trữ đảm bảo không có khả năng phục hồi.

5. Quy định trách nhiệm của cá nhân trong quản lý, sử dụng vật mang tin.

Mục 2
QUẢN LÝ NGUỒN NHÂN LỰC

Điều 11. Tuyển dụng hoặc phân công nhiệm vụ

1. Xác định trách nhiệm trong việc đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin của vị trí cần tuyển dụng hoặc phân công.

2. Khi tuyển dụng, phân công người làm việc tại các vị trí quan trọng của hệ thống công nghệ thông tin như quản trị hệ thống, quản trị hệ thống an ninh bảo mật, vận hành hệ thống, quản trị cơ sở dữ liệu, đơn vị phải xem xét, đánh giá nghiêm ngặt tư cách đạo đức, trình độ chuyên môn thông qua lý lịch, lý lịch tư pháp.

3. Yêu cầu người được tuyển dụng phải cam kết bảo mật thông tin bằng văn bản riêng hoặc cam kết trong hợp đồng lao động. Cam kết này phải bao gồm các điều khoản về trách nhiệm đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong và sau khi làm việc tại đơn vị.

4. Nhân sự mới tuyển dụng phải được đào tạo, phổ biến các quy định của đơn vị về an toàn, bảo mật hệ thống công nghệ thông tin.

Điều 12. Quản lý sử dụng nguồn nhân lực

Đơn vị có trách nhiệm thực hiện:

1. Phổ biến và cập nhật các quy định về an toàn, bảo mật hệ thống công nghệ thông tin cho tất cả cán bộ, nhân viên.

2. Kiểm tra việc thi hành các quy định về an toàn, bảo mật hệ thống công nghệ thông tin đối với cá nhân, tổ chức trực thuộc tối thiểu mỗi năm một lần.

3. Áp dụng các biện pháp xử lý kỷ luật đối với cán bộ, nhân viên của đơn vị vi phạm quy định an toàn, bảo mật hệ thống công nghệ thông tin theo quy định của pháp luật.

4. Khi cài đặt, cấu hình hệ thống, thiết bị quan trọng (máy chủ, phần mềm ứng dụng và các hệ thống an ninh mạng) trên môi trường chính thức do cán bộ, nhân viên của đơn vị thực hiện phải có biện pháp giám sát. Trường hợp thực hiện trên cơ sở dữ liệu hoặc các trường hợp do bên thứ ba thực hiện phải có cán bộ, nhân viên của đơn vị giám sát.

5. Tách biệt nhân sự giữa:

a) Phát triển và quản trị vận hành hệ thống công nghệ thông tin;

b) Quản trị cơ sở dữ liệu và phát triển ứng dụng;

c) Quản trị cơ sở dữ liệu và vận hành ứng dụng;

d) Quản trị hệ thống công nghệ thông tin chính và hệ thống công nghệ thông tin dự phòng.

6. Có biện pháp quản lý tài khoản người dùng của cán bộ, nhân viên trên các hệ thống công nghệ thông tin quan trọng khi cá nhân đó nghỉ không đến trụ sở làm việc.

7. Rà soát, kiểm tra quyền truy cập vào các hệ thống công nghệ thông tin đối với tất cả cán bộ, nhân viên đảm bảo quyền truy cập phù hợp với nhiệm vụ được giao theo định kỳ tối thiểu ba tháng một lần đối với hệ thống công nghệ thông tin quan trọng và sáu tháng một lần đối với các hệ thống công nghệ thông tin khác.

Điều 13. Chấm dứt hoặc thay đổi công việc

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

1. Xác định rõ trách nhiệm của cán bộ, nhân viên và các bên liên quan trong quản lý, vận hành và khai thác các hệ thống công nghệ thông tin.

2. Làm biên bản bàn giao tài sản công nghệ thông tin với cán bộ, nhân viên.

3. Thu hồi quyền truy cập hệ thống công nghệ thông tin của cán bộ, nhân viên nghỉ việc.

4. Thay đổi quyền truy cập hệ thống công nghệ thông tin của cán bộ, nhân viên thay đổi công việc đảm bảo nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao.

5. Rà soát, kiểm tra đối chiếu định kỳ tối thiểu ba tháng một lần giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống công nghệ thông tin để đảm bảo tài khoản người dùng của cán bộ, nhân viên đã nghỉ việc được thu hồi.

6. Thông báo cho Ngân hàng Nhà nước (Cục Công nghệ tin học) các trường hợp cá nhân làm việc trong lĩnh vực công nghệ thông tin bị kỷ luật với hình thức sa thải, buộc thôi việc hoặc bị truy tố trước pháp luật do vi phạm quy định về an toàn bảo mật hệ thống công nghệ thông tin.

Mục 3

ĐẢM BẢO AN TOÀN VỀ MẶT VẬT LÝ VÀ MÔI TRƯỜNG NƠI LẮP ĐẶT TRANG THIẾT BỊ CÔNG NGHỆ THÔNG TIN

Điều 14. Yêu cầu chung đối với nơi lắp đặt trang thiết bị công nghệ thông tin

1. Bảo vệ bằng tường bao, cổng ra vào hoặc có các biện pháp kiểm soát, hạn chế rủi ro xâm nhập trái phép.

2. Thực hiện các biện pháp phòng chống nguy cơ do cháy nổ, ngập lụt.

3. Các khu vực có yêu cầu cao về an toàn, bảo mật như khu vực lắp đặt máy chủ, thiết bị lưu trữ, thiết bị an ninh bảo mật, thiết bị truyền thông phải được cách ly với khu vực dùng chung, phân phối, chuyển hàng; ban hành nội quy, hướng dẫn làm việc và áp dụng biện pháp kiểm soát ra vào khu vực đó.

Điều 15. Yêu cầu đối với trung tâm dữ liệu

Ngoài việc đảm bảo yêu cầu tại Điều 14 Thông tư này, Trung tâm dữ liệu phải đảm bảo các yêu cầu sau:

1. Cổng/cửa vào ra trung tâm dữ liệu phải có người kiểm soát 24/7.

2. Khu vực lắp đặt thiết bị phải được tránh nắng chiếu rọi trực tiếp, chống thấm dột nước, tránh ngập lụt. Cửa vào ra phải chắc chắn, có khả năng chống cháy, sử dụng ít nhất hai loại khóa khác nhau (khóa cơ, thẻ, mã số, sinh trắc học).

3. Khu vực lắp đặt thiết bị của hệ thống công nghệ thông tin quan trọng phải được bảo vệ, giám sát 24/7.

4. Có tối thiểu một nguồn điện lưới và một nguồn điện máy phát. Có hệ thống chuyển mạch tự động giữa hai nguồn điện, khi cắt điện lưới máy phát phải tự động khởi động cấp nguồn trong thời gian tối đa ba phút. Nguồn điện phải đấu nối qua hệ thống UPS để cấp nguồn cho thiết bị, đảm bảo khả năng duy trì hoạt động của thiết bị trong thời gian tối thiểu 30 phút.

5. Có hệ thống điều hòa không khí đảm bảo khả năng hoạt động liên tục.

6. Có hệ thống chống sét trực tiếp và lan truyền.

7. Có hệ thống báo cháy và chữa cháy tự động đảm bảo khi chữa cháy không làm hư hỏng thiết bị lắp đặt bên trong.

8. Có hệ thống sàn kỹ thuật hoặc lớp cách ly chống nhiễm điện.

9. Có hệ thống camera giám sát, lưu trữ dữ liệu tối thiểu 100 ngày.

10. Có hệ thống theo dõi, kiểm soát nhiệt độ, độ ẩm.

11. Có sổ ghi nhật ký ra vào.

Điều 16. An toàn, bảo mật tài sản vật lý

1. Tài sản vật lý 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 vật lý thuộc hệ thống công nghệ thông tin quan trọng 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 đất; 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. 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 4
QUẢN LÝ VẬN HÀNH VÀ TRAO ĐỔI THÔNG TIN

Điều 17. Trách nhiệm quản lý và quy trình vận hành của các đơn vị

1. Ban hành các quy trình vận hành hệ thống công nghệ thông tin, tối thiểu bao gồm: Quy trình khởi động, đóng hệ thống; quy trình sao lưu, phục hồi dữ liệu; quy trình vận hành ứng dụng; quy trình xử lý sự cố; quy trình giám sát và ghi nhật ký hoạt động của hệ thống. Trong đó phải xác định rõ phạm vi, trách nhiệm của người sử dụng, vận hành hệ thống.

2. Kiểm soát sự thay đổi của phiên bản phần mềm, cấu hình phần cứng, quy trình vận hành: ghi chép lại các thay đổi; lập kế hoạch, thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả và phải được phê duyệt trước khi áp dụng chính thức. Có phương án dự phòng cho việc phục hồi hệ thống trong trường hợp thực hiện thay đổi không thành công hoặc gặp các sự cố không có khả năng dự tính trước.

3. Hệ thống công nghệ thông tin vận hành chính thức phải đáp ứng yêu cầu:

a) Tách biệt với môi trường phát triển và môi trường kiểm tra, thử nghiệm;

b) Áp dụng các giải pháp an ninh, an toàn;

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

4. Đối với hệ thống công nghệ thông tin xử lý giao dịch khách hàng:

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

b) Áp dụng các biện pháp đảm bảo tính toàn vẹn dữ liệu giao dịch;

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

Điều 18. Lập kế hoạch và chấp nhận hệ thống công nghệ thông tin

1. Đơn vị phải xây dựng tiêu chuẩn, định mức, yêu cầu kỹ thuật để đảm bảo hệ thống hệ công nghệ thông tin hoạt động bình thường đối với tất cả các hệ thống hiện có và các hệ thống công nghệ thông tin trước khi đưa vào áp dụng chính thức.

2. Căn cứ các tiêu chuẩn, định mức, yêu cầu kỹ thuật đã xây dựng, đơn vị thực hiện giám sát, tối ưu hiệu suất của hệ thống công nghệ thông tin; đánh giá khả năng đáp ứng của hệ thống công nghệ thông tin để dự báo, lập kế hoạch mở rộng, nâng cấp đảm bảo khả năng đáp ứng trong tương lai.

3. Đơn vị phải rà soát, cập nhật tiêu chuẩn, định mức, yêu cầu kỹ thuật khi có sự thay đổi đối với hệ thống công nghệ thông tin. Thực hiện đào tạo và chuyển giao kỹ thuật đối với những nội dung thay đổi cho các nhân sự có liên quan.

Điều 19. Sao lưu dự phòng

1. Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo mức độ quan trọng, 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. Yêu cầu dữ liệu của các hệ thống công nghệ thông tin quan trọng phải được sao lưu trong ngày.

2. Dữ liệu của các hệ thống công nghệ thông tin quan trọng phải được sao lưu ra phương tiện lưu trữ ngoài (như băng từ, đĩa cứng, đĩa quang hoặc phương tiện lưu trữ khác) và cất giữ, bảo quản an toàn tách rời với khu vực tiến hành sao lưu. Kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu sáu tháng một lần.

3. Các đơn vị có cả hệ thống công nghệ thông tin chính và dự phòng đặt ngoài lãnh thổ Việt Nam phải sao lưu hàng ngày đối với dữ liệu điện tử về các hoạt động giao dịch và lưu trữ tại Việt Nam. Đơn vị phải đảm bảo khả năng chuyển đổi dữ liệu gốc từ bản dữ liệu sao lưu. Kiểm tra, chuyển đổi dữ liệu sao lưu tối thiểu sáu tháng một lần.

Điều 20. Quản lý về an toàn, bảo mật mạng

1. Xây dựng quy định về quản lý an toàn, bảo mật mạng và quản lý các thiết bị đầu cuối của toàn bộ hệ thống mạng.

2. Hệ thống mạng phải được chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng và hệ thống thông tin. Các vùng mạng quan trọng phải được lắp đặt các thiết bị tường lửa để kiểm soát an toàn bảo mật.

3. Lập, lưu trữ hồ sơ về sơ đồ logic và vật lý đối với hệ thống mạng máy tính, bao gồm cả mạng diện rộng (WAN/Intranet) và mạng cục bộ (LAN).

4. Trang bị các giải pháp an ninh mạng để kiểm soát, phát hiện và ngăn chặn kịp thời các kết nối, truy cập không được phép vào hệ thống mạng.

5. Thiết lập, cấu hình đầy đủ các tính năng của hệ thống an ninh mạng. Thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

Điều 21. Trao đổi thông tin

Đơn vị có trách nhiệm:

1. Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông tin; biện pháp đảm bảo tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

2. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính hoặc vật mang tin.

3. Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho khách hàng.

4. Có văn bản thỏa thuận cho việc trao đổi thông tin với bên ngoài. Xác định trách nhiệm và nghĩa vụ pháp lý của các bên tham gia.

5. Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

Điều 22. Quản lý dịch vụ giao dịch trực tuyến

1. Yêu cầu đối với hệ thống công nghệ thông tin phục vụ cho việc cung cấp dịch vụ giao dịch trực tuyến cho khách hàng:

a) Phải đảm bảo tính sẵn sàng cao và có khả năng phục hồi nhanh chóng;

b) Dữ liệu trên đường truyền phải được mã hóa và phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép;

c) Xác thực giao dịch bằng tối thiểu hai yếu tố. Đối với các giao dịch giá trị cao phải xác thực bằng các phương thức xác thực mạnh như sinh trắc học (vân tay, tĩnh mạch ngón tay hoặc bàn tay, mống mắt, giọng nói, khuôn mặt) hoặc chữ ký số;

d) Trang thông tin điện tử giao dịch trực tuyến phải được chứng thực chống giả mạo và phải được áp dụng các biện pháp bảo vệ nhằm ngăn chặn, chống sửa đổi trái phép.

2. Xác thực giao dịch của khách hàng phải được thực hiện trực tiếp tại hệ thống công nghệ thông tin của đơn vị.

3. Kiểm soát chặt chẽ việc truy cập vào hệ thống giao dịch trực tuyến từ bên trong mạng nội bộ.

4. Hệ thống dịch vụ giao dịch trực tuyến phải được giám sát chặt chẽ có khả năng phát hiện, cảnh báo về:

a) Các giao dịch đáng ngờ, gian lận dựa vào việc xác định thời gian, vị trí địa lý, tần suất giao dịch, số tiền giao dịch, số lần xác thực sai quy định và các dấu hiệu bất thường khác;

b) Hoạt động bất thường của hệ thống;

c) Các cuộc tấn công từ chối dịch vụ (DoS - Denial of Service attack), tấn công từ chối dịch vụ phân tán (DDoS - Distributed Denial of Service attack).

5. Thông tin nhạy cảm của khách hàng (mã PIN và mã khóa bí mật) phải được mã hóa ở lớp ứng dụng.

6. Khách hàng trước khi tham gia sử dụng dịch vụ giao dịch trực tuyến phải được cảnh bảo rủi ro, hướng dẫn các biện pháp an toàn, bảo mật.

7. Không cung cấp phần mềm ứng dụng giao dịch trực tuyến trên Internet khi chưa áp dụng các biện pháp đảm bảo an toàn, bảo mật cho khách hàng.

Điều 23. Giám sát và ghi nhật ký hoạt động của hệ thống công nghệ thông tin

1. Ghi và lưu trữ nhật ký về hoạt động của hệ thống công nghệ thông tin và người sử dụng, các lỗi phát sinh, các sự cố mất an toàn hệ thống công nghệ thông tin. Dữ liệu nhật ký phải được lưu trữ trực tuyến tối thiểu ba tháng và sao lưu tối thiểu một năm.

2. Thực hiện các biện pháp giám sát, phân tích nhật ký, cảnh báo rủi ro, xử lý và báo cáo kết quả.

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. Thực hiện việc đồng bộ thời gian giữa các hệ thống công nghệ thông tin.

Điều 24. Phòng chống mã độc

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

1. Xác định trách nhiệm của người sử dụng và các bộ phận liên quan trong công tác phòng chống mã độc.

2. Triển khai biện pháp, giải pháp phòng chống mã độc cho toàn bộ hệ thống công nghệ thông tin của đơn vị.

3. Cập nhật mẫu mã độc và phần mềm phòng chống mã độc mới.

4. Kiểm tra, diệt mã độc đối với vật mang tin nhận từ bên ngoài trước khi sử dụng.

5. Kiểm soát việc cài đặt phần mềm đảm bảo tuân thủ theo quy chế an toàn, bảo mật của đơn vị.

6. Kiểm soát thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ.

Mục 5
CÁC BIỆN PHÁP QUẢN LÝ TRUY CẬP

Điều 25. Yêu cầu nghiệp vụ đối với kiểm soát truy cập

1. Quy định về quản lý truy cập đối với người sử dụng, nhóm người sử dụng, các thiết bị, công cụ sử dụng để truy cập đảm bảo đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn, bảo mật, 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 sử dụng tài khoản quản trị hệ thống công nghệ thông tin;

c) Quản lý, cấp phát mã khóa bí mật về truy cập mạng, hệ điều hành, truy cập hệ thống thông tin và ứng dụng;

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

đ) Yêu cầu, điều kiện an toàn, bảo mật đối với các thiết bị, công cụ sử dụng để truy cập.

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

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

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

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

3. Quy định trách nhiệm người sử dụng khi được cấp quyền truy cập: Sử dụng mã khóa bí mật đúng quy định, giữ bí mật mã khóa bí mật, sử dụng thiết bị, công cụ để truy cập theo đúng quy định, thoát khỏi hệ thống khi không làm việc trên hệ thống hoặc tạm thời không làm việc trên hệ thống.

Điều 26. Quản lý truy cập mạng nội bộ

1. Quy định quản lý truy cập mạng và các dịch vụ mạng gồm các nội dung cơ bản sau:

a) Các mạng và dịch vụ mạng được phép sử dụng, cách thức, phương tiện và các điều kiện an toàn bảo mật để truy cập;

b) Trách nhiệm của người quản trị, người truy cập;

c) Thủ tục cấp phát, thay đổi, thu hồi quyền kết nối;

d) Kiểm soát việc quản trị, truy cập, sử dụng mạng.

2. Thực hiện các biện pháp kiểm soát chặt chẽ các kết nối từ bên ngoài vào mạng nội bộ của đơn vị đảm bảo an toàn, bảo mật.

3. Kiểm soát việc cài đặt, sử dụng các công cụ phần mềm hỗ trợ truy cập từ xa.

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

5. Cấp quyền truy cập mạng và dịch vụ mạng phải đảm bảo nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao.

Điều 27. Quản lý truy cập hệ điều hành

1. 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.

2. Yêu cầu sử dụng biện pháp xác thực đa thành tố, tên định danh/mã khóa bí mật và thành tố khác (như sinh trắc học hoặc thẻ hoặc mật khẩu dùng một lần,...) đối với truy cập từ xa vào các hệ thống công nghệ thông tin quan trọng, tối thiểu bao gồm hệ thống máy chủ, thiết bị mạng và an ninh bảo mật.

3. 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.

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

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

Điều 28. Quản lý truy cập Internet

1. Quy định quản lý kết nối, truy cập sử dụng Internet gồm các nội dung cơ bản sau:

a) Trách nhiệm cá nhân và các bộ phận có liên quan trong khai thác sử dụng Internet;

b) Đối tượng người dùng được phép truy cập, kết nối sử dụng Internet;

c) Các hành vi bị cấm, hạn chế;

d) Kiểm soát kết nối, truy cập sử dụng Internet;

đ) Các biện pháp đảm bảo an toàn thông tin khi kết nối Internet.

2. Thực hiện quản lý tập trung, thống nhất các cổng kết nối Internet trong toàn đơn vị. Phải kiểm soát các truy cập của khách hàng ra Internet thông qua cổng kết

nối do đơn vị cung cấp.

3. Triển khai các giải pháp an ninh mạng tại các cổng kết nối Internet để đảm bảo an toàn trước các hiểm họa tấn công từ Internet vào mạng nội bộ của đơn vị.

4. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các tấn công, truy cập bất hợp pháp vào hệ thống mạng nội bộ của đơn vị thông qua cổng kết nối Internet.

Điều 29. Kiểm soát truy cập thông tin và ứng dụng

1. Quản lý và phân quyền truy cập thông tin và ứng dụng đảm bảo nguyên tắc cấp quyền vừa đủ để thực hiện nhiệm vụ được giao 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. Các hệ thống thông tin cùng sử dụng nguồn tài nguyên chung phải được người quản trị hệ thống chấp nhận.

Mục 6
QUẢN LÝ DỊCH VỤ CÔNG NGHỆ THÔNG TIN CỦA BÊN THỨ BA

Điều 30. Ký kết hợp đồng với bên thứ ba

Đơn vị phải thực hiện:

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 hoá, dịch vụ.

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

3. Xác định, đánh giá các rủi ro có thể phát sinh và áp dụng các biện pháp quản lý rủi ro đối với hệ thống công nghệ thông tin của đơn vị liên quan tới việc thực hiện hợp đồng của bên thứ ba.

4. Đơn vị không được thuê bên thứ ba thực hiện toàn bộ công việc quản trị (chỉnh sửa cấu hình, dữ liệu, nhật ký) đối với các hệ thống công nghệ thông tin quan trọng.

Điều 31. Trách nhiệm của đơn vị trong quản lý các dịch vụ do bên thứ ba cung cấp

1. Cung cấp, thông báo và yêu cầu bên thứ ba thực hiện các quy định của đơn vị về an toàn bảo mật hệ thống công nghệ thông tin.

2. 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.

3. 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.

4. 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.

5. 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 do bên thứ ba cung cấp.

6. 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 công nghệ thông tin của đơn vị.

7. Giám sát nhân sự của bên thứ ba trong quá trình thực hiện hợp đồng. Khi phát hiện nhân sự bên thứ ba vi phạm quy định về an toàn bảo mật phải thông báo và phối hợp với bên thứ ba áp dụng biện pháp xử lý kịp thời.

8. Thu hồi quyền truy cập hệ thống công nghệ thông tin đã được cấp cho bên thứ ba, thay đổi các khoá, mã khóa bí mật nhận bàn giao từ bên thứ ba ngay sau khi hoàn thành công việc hoặc kết thúc hợp đồng.

Điều 32. Trách nhiệm của bên thứ ba khi cung cấp dịch vụ công nghệ thông tin

1. Ký và thực hiện cam kết bảo mật thông tin cả trong quá trình triển khai và sau khi hoàn tất hợp đồng.

2. Lập kế hoạch, bố trí nhân sự và các nguồn lực khác để thực hiện hợp đồng. Thông báo danh sách nhân sự triển khai cho bên ký kết hợp đồng và phải được đơn vị chấp thuận. Nhân sự bên thứ ba phải ký cam kết không tiết lộ thông tin quan trọng của bên ký kết hợp đồng.

3. Phổ biến các quy định, quy chế an toàn bảo mật của bên ký kết hợp đồng cho nhân sự tham gia triển khai và thực hiện biện pháp giám sát đảm bảo sự tuân thủ. Tạm dừng hoặc đình chỉ hoạt động, thu hồi quyền truy cập và thông báo ngay cho bên ký kết hợp đồng khi phát hiện nhân sự vi phạm quy định về an toàn bảo mật. Bồi thường thiệt hại do nhân sự tham gia thực hiện hợp đồng gây ra.

4. Hồ sơ nghiệm thu hợp đồng phải bao gồm báo cáo chi tiết về mặt kỹ thuật, hồ sơ hoàn công lắp đặt thiết bị, cấu hình phần mềm, hướng dẫn vận hành (nếu có) theo các nội dung công việc bên thứ ba đã thực hiện.

5. Bàn giao tài sản, quyền truy cập hệ thống công nghệ thông tin do bên ký kết hợp đồng cung cấp khi hoàn thành công việc hoặc kết thúc hợp đồng.

Mục 7

TIẾP NHẬN, PHÁT TRIỂN, DUY TRÌ HỆ THỐNG CÔNG NGHỆ THÔNG TIN

Điều 33. Yêu cầu về an toàn, bảo mật cho các hệ thống công nghệ thông tin

Khi xây dựng mới hoặc cải tiến hệ thống công nghệ thông tin, đơn vị phải:

1. Xây dựng các yêu cầu về an toàn, bảo mật đồng thời với việc đưa ra các yêu cầu kỹ thuật, nghiệp vụ.

2. Đánh giá mức độ đáp ứng các yêu cầu về an toàn, bảo mật sau khi hoàn thành xây dựng hoặc cải tiến hệ thống công nghệ thông tin. Kết quả đánh giá phải lập thành báo cáo và được thủ trưởng đơn vị phê duyệt trước khi đưa vào vận hành chính thức.

Điều 34. Đảm bảo an toàn, bảo mật các ứng dụng

Các chương trình ứng dụng nghiệp vụ phải đạt các yêu cầu tối thiểu 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.

5. Mã khóa bí mật của người sử dụng trong các hệ thống công nghệ thông tin quan trọng phải được mã hóa ở lớp ứng dụng.

Điều 35. Quản lý mã hóa

1. Quy định và đưa vào sử dụng các biện pháp mã hóa theo các chuẩn quốc gia hoặc quốc tế đã được công nhận, có biện pháp quản lý khóa 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 mã khóa bí mật khách hàng, mã khóa bí mật người sử dụng và

các dữ liệu nhạy cảm khác phải được mã hóa, bảo vệ khi truyền trên mạng và khi lưu trữ.

Điều 36. An toàn, bảo mật đối với chương trình nguồn, dữ liệu kiểm thử và các tệp tin cấu hình hệ thống

1. Đơn vị phải có quy định về:

a) Quản lý, kiểm soát chương trình nguồn. Việc truy cập, tiếp cận chương trình nguồn phải được sự phê duyệt của thủ trưởng đơn vị.

b) Quản lý, bảo vệ tệp tin cấu hình hệ thống.

2. Đơn vị phải xây dựng quy trình lựa chọn, quản lý và kiểm soát đối với dữ liệu kiểm tra, thử nghiệm. Không sử dụng dữ liệu thật của hệ thống công nghệ thông tin vận hành chính thức cho hoạt động kiểm thử khi chưa thực hiện các biện pháp che giấu hoặc thay đổi đối với dữ liệu nhạy cảm.

Điều 37. Quản lý sự thay đổi hệ thống công nghệ thông tin

Ban hành quy trình, biện pháp quản lý và kiểm soát sự thay đổi hệ thống công nghệ thông tin, tối thiểu bao gồm:

1. 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.

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

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

Điều 38. Đánh giá an ninh bảo mật hệ thống công nghệ thông tin

1. Đơn vị phải thực hiện đánh giá an ninh bảo mật hệ thống công nghệ thông tin với các nội dung cơ bản sau:

a) Đánh giá về kiến trúc hệ thống để xác định tính phù hợp của các thiết bị lắp đặt với kiến trúc hệ thống tổng thể và yêu cầu về an ninh bảo mật;

b) Đánh giá tình trạng hoạt động, cấu hình hệ thống công nghệ thông tin đảm bảo hệ thống hoạt động theo các tiêu chuẩn, định mức, yêu cầu kỹ thuật quy định tại Khoản 1 Điều 18 Thông tư này;

c) Kiểm tra cấu hình các thiết bị bảo mật, các hệ thống cấp quyền truy cập tự động, hệ thống quản lý thiết bị đầu cuối, danh sách tài khoản người dùng;

d) Kiểm tra thử nghiệm mức độ an toàn mạng (Penetration Test), bắt buộc phải thực hiện đối với các hệ thống công nghệ thông tin có kết nối và cung cấp thông tin, dịch vụ ra Internet.

2. Định kỳ thực hiện đánh giá an ninh bảo mật hệ thống công nghệ thông tin, tối thiểu như sau:

a) Sáu tháng một lần đối với các trang thiết bị giao tiếp trực tiếp với môi trường bên ngoài như Internet, kết nối với khách hàng và bên thứ ba theo các nội

dung tại Điểm b, c, d của Khoản 1 Điều này;

b) Mỗi năm một lần đối với hệ thống công nghệ thông tin quan trọng, hai năm một lần đối với hệ thống công nghệ thông tin khác theo các nội dung tại Khoản 1 Điều này.

3. Kết quả đánh giá phải được lập thành văn bản báo cáo thủ trưởng đơn vị. Đối với các nội dung chưa tuân thủ quy định về an toàn bảo mật trong hoạt động công nghệ thông tin (nếu có) phải đề xuất biện pháp, kế hoạch, thời hạn xử lý, khắc phục.

Điều 39. 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 về mặt kỹ thuật của các hệ thống công nghệ thông tin đang sử dụng.

2. Đơn vị phải chủ động phát hiện các điểm yếu về mặt kỹ thuật:

a) Thường xuyên cập nhật thông tin liên quan đến lỗ hổng, điểm yếu về mặt kỹ thuật;

b) Thực hiện dò quét, phát hiện các lỗ hổng, điểm yếu về mặt kỹ thuật của các hệ thống công nghệ thông tin đang sử dụng tối thiểu ba tháng một lần đối với các hệ thống có kết nối với môi trường bên ngoài, sáu tháng một lần đối với các hệ thống khác.

3. Đánh giá mức độ tác động, rủi ro của từng lỗ hổng, điểm yếu về mặt kỹ thuật được phát hiện đối với hệ thống công nghệ thông tin đang sử dụng và đưa ra phương án xử lý.

4. Xây dựng, tổ chức triển khai các giải pháp xử lý, khắc phục và báo cáo kết quả xử lý.

Mục 8
QUẢN LÝ CÁC SỰ CỐ VỀ CÔNG NGHỆ THÔNG TIN

Điều 40. Quy trình xử lý sự cố

1. Tiếp nhận thông tin về sự cố phát sinh.

2. Đánh giá xác định mức độ, phạm vi ảnh hưởng của sự cố đến hoạt động của hệ thống công nghệ thông tin. Tùy theo mức độ, phạm vi ảnh hưởng của sự cố phải báo cáo đến các cấp quản lý tương ứng để chỉ đạo xử lý.

3. Thực hiện các biện pháp xử lý, khắc phục sự cố.

4. Ghi nhận hồ sơ và báo cáo kết quả xử lý sự cố.

5. Quy định trách nhiệm của cá nhân, tập thể trong việc báo cáo, tiếp nhận, xử lý các sự cố về công nghệ thông tin.

6. Xây dựng các mẫu biểu để ghi nhận, lưu trữ hồ sơ xử lý sự cố.

Điều 41. Kiểm soát và khắc phục sự cố

1. Các sự cố mất an toàn hệ thống công nghệ thông tin 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.

2. Đánh giá xác định nguyên nhân và thực hiện các biện pháp phòng ngừa tránh sự cố tái diễn.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị. Thực hiện biện pháp bảo vệ, chống chỉnh sửa, hủy hoại đối với tài liệu về sự cố được lưu trữ.

4. 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 công nghệ thông tin 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 CÔNG NGHỆ THÔNG TIN

Điều 42. Xây dựng hệ thống dự phòng thảm họa

1. Đơn vị phải xây dựng hệ thống dự phòng thảm họa cho các hệ thống công nghệ thông tin quan trọng đáp ứng các yêu cầu sau:

a) Địa điểm lắp đặt phải cách hệ thống chính tối thiểu 20 km tính theo đường thẳng nối giữa hai hệ thống và phải đáp ứng các yêu cầu quy định tại Điều 14 Thông tư này;

b) Từng hệ thống dự phòng phải đảm bảo khả năng thay thế hệ thống chính trong thời gian tối đa bốn giờ đồng hồ tính từ thời điểm hệ thống chính có sự cố không khắc phục được.

2. Các đơn vị chỉ có hệ thống công nghệ thông tin tại một địa điểm duy nhất ở Việt Nam phải xây dựng hệ thống dự phòng thảm hoạ tại một địa điểm khác đáp ứng yêu cầu nêu tại Điểm a Khoản 1 Điều này.

3. Kế hoạch xây dựng hệ thống dự phòng thảm hoạ:

a) Đối với các tổ chức tín dụng, các chi nhánh ngân hàng nước ngoài phải hoàn thành trong thời gian sáu tháng kể từ ngày Thông tư này có hiệu lực;

b) Đối với các tổ chức cung ứng dịch vụ trung gian thanh toán phải hoàn thành trong thời gian mười hai tháng kể từ ngày Thông tư này có hiệu lực.

Điều 43. Xây dựng quy trình, kịch bản đảm bảo hoạt động liên tục

1. Xây dựng quy trình xử lý các tình huống mất an toàn, gián đoạn hoạt động của từng cấu phần trong hệ thống công nghệ thông tin quan trọng như máy chủ, thiết bị mạng, an ninh bảo mật, truyền thông.

2. Xây dựng kịch bản chuyển đổi hệ thống dự phòng thay thế cho hoạt động của hệ thống chính, bao gồm các nội dung cơ bản sau:

a) Nội dung công việc, trình tự thực hiện, dự kiến thời gian hoàn thành;

b) Bố trí và phân công trách nhiệm cho nhân sự tham gia với các vai trò: Chỉ đạo thực hiện, giám sát, thực hiện chuyển đổi, kiểm tra kết quả chuyển đổi và vận hành thử nghiệm;

c) Các nguồn lực, phương tiện và các yêu cầu cần thiết để thực hiện;

d) Biện pháp đảm bảo an toàn, bảo mật thông tin và hệ thống công nghệ thông tin;

đ) Các mẫu biểu ghi nhận kết quả.

3. Các đơn vị chỉ có hệ thống công nghệ thông tin tại một địa điểm duy nhất ở Việt Nam phải xây dựng kịch bản chuyển đổi hoạt động hệ thống công nghệ thông tin sang hệ thống dự phòng nêu tại Khoản 2 Điều 42 Thông tư này.

4. Kịch bản chuyển đổi phải được phổ biến tới tất cả các đối tượng tham gia để nắm rõ nội dung công việc cần thực hiện.

5. Quy trình, kịch bản chuyển đổi phải được kiểm tra và cập nhật khi có sự thay đổi của hệ thống công nghệ thông tin, cơ cấu tổ chức, nhân sự và phân công trách nhiệm của các bộ phận có liên quan trong đơn vị.

Điều 44. Tổ chức triển khai diễn tập đảm bảo hoạt động liên tục

1. Đơn vị phải có kế hoạch và tổ chức triển khai diễn tập đảm bảo hoạt động liên tục hệ thống công nghệ thông tin:

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

b) Tối thiểu sáu tháng một lần, phải thực hiện diễn tập chuyển hoạt động của từng hệ thống từ hệ thống chính sang hệ thống dự phòng theo kịch bản đã xây dựng tại Điều 43 Thông tư này. Đánh giá kết quả và cập nhật các quy trình, kịch bản diễn tập (nếu có).

2. Thông báo kế hoạch diễn tập cho Ngân hàng Nhà nước (Cục Công nghệ tin học) chậm nhất là 05 (năm) ngày làm việc trước khi chuyển hoạt động từ hệ thống chính sang hệ thống dự phòng (bao gồm cả các đơn vị không đặt hệ thống công nghệ thông tin chính và dự phòng tại Việt Nam).

Mục 10

KIỂM TRA NỘI BỘ VÀ CHẾ ĐỘ BÁO CÁO

Điều 45. Kiểm tra nội bộ

1. Xây dựng quy định kiểm tra nội bộ về công tác đảm bảo an toàn bảo mật hoạt động công nghệ thông tin của đơn vị.

2. Xây dựng kế hoạch và thực hiện công tác tự tổ chức kiểm tra việc tuân thủ các quy định tại Thông tư này và các quy định của đơn vị về đảm bảo an toàn bảo mật hoạt động công nghệ thông tin tối thiểu mỗi năm một lần.

3. Kết quả kiểm tra về công tác đảm bảo an toàn bảo mật hoạt động công nghệ thông tin của đơn vị phải lập thành báo cáo gửi thủ trưởng đơn vị, trong đó các vấn đề còn tồn tại chưa đảm bảo tuân thủ các quy định về an toàn bảo mật hoạt động công nghệ thông tin (nếu có) phải kiến nghị, đề xuất xử lý, khắc phục.

4. Tổ chức thực hiện và báo cáo kết quả xử lý, khắc phục các tồn tại nêu trong báo cáo theo quy định tại Khoản 3 Điều này.

Điều 46. Chế độ báo cáo

Đơn vị (trừ Ngân hàng Nhà nước) có trách nhiệm gửi báo cáo về Ngân hàng Nhà nước (Cục Công nghệ tin học) bằng văn bản tiếng Việt như sau:

1. Báo cáo năm

a) Nội dung báo cáo:

- Việc thực hiện đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin theo quy định tại Thông tư này;

- Các nội dung chỉnh sửa, bổ sung quy chế an toàn, bảo mật hệ thống công nghệ thông tin của đơn vị (nếu có).

b) Thời hạn gửi báo cáo: trước ngày 31 tháng 01 của năm tiếp theo;

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

2. Báo cáo đột xuất

a) Các sự cố mất an toàn hệ thống công nghệ thông tin:

- Thời hạn gửi báo cáo: trong thời gian 01 (một) ngày kể từ thời điểm vụ, việc được phát hiện;

- Nội dung vụ, việc;

- Thời gian, địa điểm phát sinh vụ, việc;

- Nguyên nhân xảy ra vụ, việc (nếu có);

- Đánh giá rủi ro, ảnh hưởng đối với hệ thống công nghệ thông tin 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.

b) Triển khai mới, nâng cấp và đưa vào ứng dụng các hệ thống công nghệ thông tin quan trọng:

- Thời hạn gửi báo cáo: Chậm nhất 05 (năm) ngày trước khi áp dụng chính thức;

- Hệ thống, ứng dụng dự kiến triển khai;

- Phạm vi áp dụng;

- Kết quả kiểm tra, kiểm thử;

- Kế hoạch triển khai thực hiện;

- Đánh giá rủi ro, mức độ ảnh hưởng của hệ thống mới đối với các hệ thống công nghệ thông tin hiện có của đơn vị;

- Đề xuất, kiến nghị.

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

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 47. 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 48. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 01/03/2016 và thay thế Thông tư 01/2011/TT-NHNN ngày 21/02/2011 của Thống đốc Ngân hàng Nhà nước Việt Nam về việc ban hành Quy định việc đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong ngành Ngân hàng.

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 49. Trách nhiệm thi hành

1. Cục Công nghệ tin học có trách nhiệm:

a) Xây dựng các tiêu chuẩn kỹ thuật để chuẩn hóa hoạt động công nghệ thông tin của ngành ngân hàng;

b) Theo dõi, tổng hợp báo cáo Thống đốc tình hình thực hiện đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin của các đơn vị theo quy định tại Thông tư này;

c) Hàng năm lập kế hoạch và kiểm tra việc thực hiện Thông tư này tại các đơn vị;

d) 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 việc thực hiện Thông tư này tại các đơn vị (trừ Ngân hàng Nhà nước) 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 việc kiểm tra nội bộ đối với các đơn vị thuộc Ngân hàng Nhà nước theo quy định tại Khoản 1, 2, 3 Điều 45 Thông tư này.

4. Thủ trưởng các đơn vị liên quan thuộc Ngân hàng Nhà nước; Giám đốc Ngân hàng Nhà nước chi nhánh tỉnh, thành phố trực thuộc trung ương; Chủ tịch Hội đồng quản trị, 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 có trách nhiệm tổ chức thực hiện Thông tư này./.

Nơi nhận:
- Như Khoản 4 Điều 49;
- Ban lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Lưu VP, CNTH, PC.

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Nguyễn Toàn Thắng