NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 18 /2018/TT-NHNN	*Hà Nội, ngày 21 tháng 8 năm 2018*

THÔNG TƯ
Quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng

Căn cứ Luật Ngân hàng Nhà nước Việt Nam ngày 16 tháng 6 năm 2010;

Căn cứ Luật các tổ chức tín dụng ngày 16 tháng 6 năm 2010 và Luật sửa đổi, bổ sung một số điều của Luật các tổ chức tín dụng ngày 20 tháng 11 năm 2017;

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 16/2017/NĐ-CP ngày 17 tháng 02 năm 2017 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 thông tin;

Thống đốc Ngân hàng Nhà nước Việt Nam ban hành Thông tư quy định về an toàn hệ thống 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 bảo đảm an toàn hệ thống thông tin trong hoạt động ngân hàng.

2. Thông tư này áp dụng đối với các tổ chức tín dụng (trừ quỹ tín dụng nhân dân, 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 tổ chức).

Điều 2. Giải thích từ ngữ

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

1. Hệ thống thông tin là một tập hợp các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng để tạo lập, 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 tổ chức.

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

3. 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.

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

5. An toàn thông tin là sự bảo vệ thông tin số, hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin.

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 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. Sự cố an ninh mạng (cybersecurity incident) là việc thông tin số, hệ thống thông tin bị tấn công hoặc bị gây nguy hại, ảnh hưởng tới tính bí mật, tính toàn vẹn, tính sẵn sàng.

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

9. 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 xử lý, lưu trữ, trao đổi và quản lý tập trung dữ liệu.

10. Thiết bị di động là thiết bị số được thiết kế có thể di chuyển mà không ảnh hưởng tới khả năng hoạt động, 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.

11. Vật mang tin là các phương tiện vật chất dùng để lưu giữ và truyền nhận thông tin số.

12. 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.

13. Mạng không tin cậy là mạng bên ngoài có kết nối vào mạng của tổ chức và không thuộc sự quản lý của tổ chức hoặc không thuộc sự quản lý của tổ chức tín dụng nước ngoài mà tổ chức có quan hệ như là đơn vị phụ thuộc, hiện diện thương mại tại Việt Nam.

14. Dịch vụ điện toán đám mây là các dịch vụ cung cấp tài nguyên máy tính (computing resources) qua môi trường mạng cho phép nhiều đối tượng sử dụng, có

thể điều chỉnh và thanh toán theo nhu cầu sử dụng.

15. Tài khoản người sử dụng (tài khoản) là một tập hợp thông tin đại diện duy nhất cho người sử dụng trên hệ thống thông tin, được sử dụng để đăng nhập và truy cập các tài nguyên được cấp phép trên hệ thống thông tin đó.

16. Bên thứ ba là các cá nhân, doanh nghiệp (không bao gồm tổ chức tín dụng nước ngoài và các thành viên thuộc tổ chức tín dụng nước ngoài trong trường hợp tổ chức là đơn vị phụ thuộc, hiện diện thương mại tại Việt Nam của tổ chức tín dụng nước ngoài) có thỏa thuận bằng văn bản (gọi chung là hợp đồng sử dụng dịch vụ) với tổ chức nhằm cung cấp dịch vụ công nghệ thông tin.

17. Cấp có thẩm quyền là chức danh hoặc người được người đại diện hợp pháp của tổ chức phân cấp quản lý, phân công, ủy quyền bằng văn bản để thực hiện một hoặc một số chức năng, nhiệm vụ của tổ chức.

Điều 3. Nguyên tắc chung

1. Tổ chức có trách nhiệm bảo đảm an toàn thông tin theo nguyên tắc xác định rõ quyền hạn, trách nhiệm từng bộ phận và cá nhân trong tổ chức.

2. Phân loại hệ thống thông tin theo mức độ quan trọng và áp dụng chính sách an toàn thông tin 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 tổ chức.

4. Xây dựng, triển khai quy chế an toàn thông tin trên cơ sở các quy định tại Thông tư này và hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của tổ chức.

Điều 4. Phân loại thông tin và hệ thống thông tin

1. Thông tin xử lý, lưu trữ thông qua hệ thống thông tin được phân loại theo thuộc tính bí mật như sau:

a) Thông tin công cộng là thông tin được công khai cho tất cả các đối tượng mà không cần xác định danh tính, địa chỉ cụ thể của các đối tượng đó;

b) Thông tin nội bộ là thông tin của tổ chức được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng trong tổ chức được xác định danh tính;

c) Thông tin bí mật là thông tin: (i) Được xếp ở mức Mật theo quy định của tổ chức và hạn chế đối tượng được tiếp cận; (ii) Mật, Tối Mật, Tuyệt Mật theo quy định của pháp luật về bảo vệ bí mật nhà nước.

2. Tiêu chí phân loại theo mức độ quan trọng hệ thống thông tin của các tổ chức:

a) Hệ thống thông tin thông thường (mức độ 1) là hệ thống thông tin phục vụ

hoạt động nội bộ của tổ chức hoặc phục vụ khách hàng nhưng không xử lý thông tin bí mật;

b) Hệ thống thông tin quan trọng (mức độ 2) là hệ thống thông tin có một trong các tiêu chí sau: (i) Hệ thống thông tin có xử lý thông tin bí mật; (ii) Hệ thống thông tin phục vụ hoạt động nội bộ hàng ngày của tổ chức và không chấp nhận ngừng vận hành quá 4 giờ làm việc; (iii) Hệ thống thông tin phục vụ khách hàng yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước; (iv) Hệ thống thông tin cung cấp dịch vụ giao dịch trực tuyến cho khách hàng;

c) Hệ thống thông tin đặc biệt quan trọng (mức độ 3) là hệ thống thông tin có một trong các tiêu chí sau: (i) Hệ thống thông tin quốc gia trong ngành Ngân hàng phục vụ phát triển Chính phủ điện tử, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước; (ii) Hệ thống cơ sở hạ tầng thông tin dùng chung trong ngành Ngân hàng phục vụ hoạt động của các cơ quan, tổ chức trên phạm vi toàn quốc yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước;

d) Trong trường hợp hệ thống thông tin bao gồm nhiều hệ thống thành phần, mỗi hệ thống thành phần lại tương ứng với một mức độ quan trọng khác nhau, thì phân loại hệ thống thông tin xác định theo mức độ quan trọng của hệ thống thành phần cung cấp hoạt động kỹ thuật, nghiệp vụ chính.

3. Tổ chức thực hiện phân loại hệ thống thông tin theo mức độ quan trọng quy định tại khoản 2 Điều này. Danh sách hệ thống thông tin theo mức độ quan trọng phải được người đại diện hợp pháp phê duyệt.

Điều 5. Quy chế an toàn thông tin

1. Tổ chức xây dựng quy chế an toàn thông tin phù hợp với hệ thống thông tin, cơ cấu tổ chức, yêu cầu quản lý và hoạt động của tổ chức. Quy chế an toàn thông tin phải được người đại diện hợp pháp ký ban hành và triển khai thực hiện trong toàn tổ chức.

2. Quy chế an toàn thông tin tối thiểu gồm các nội dung cơ bản sau:

a) Quản lý tài sản công nghệ thông tin;

b) Quản lý nguồn nhân lực;

c) Bảo đảm an toàn về mặt vật lý và môi trường lắp đặt;

d) Quản lý vận hành và trao đổi thông tin;

đ) Quản lý truy cập;

e) Quản lý sử dụng 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 an toàn thông tin;

i) Bảo đảm hoạt động liên tục của hệ thống thông tin;

k) Kiểm tra nội bộ và chế độ báo cáo.

3. Tổ chức rà soát quy chế an toàn thông tin tối thiểu mỗi năm một lần, bảo đảm 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 thông tin hoặc theo yêu cầu của cơ quan có thẩm quyền, tổ chức tiến hành chỉnh sửa, bổ sung ngay quy chế an toàn thông tin đã ban hành.

Chương II
CÁC QUY ĐỊNH VỀ BẢO ĐẢM AN TOÀN THÔNG TIN
Mục 1
QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

Điều 6. Quản lý tài sản công nghệ thông tin

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

a) Tài sản thông tin: các dữ liệu, thông tin ở dạng số được xử lý, lưu trữ thông qua hệ thống thông tin;

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

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

2. Tổ chức lập danh sách của tất cả các tài sản công nghệ thông tin gắn với từng hệ thống thông tin theo quy định tại khoản 3, Điều 4 Thông tư này. Định kỳ hàng năm rà soát và cập nhật danh sách tài sản công nghệ thông tin.

3. Căn cứ theo mức độ quan trọng của hệ thống thông tin, tổ chức thực hiện các biện pháp quản lý, bảo vệ phù hợp với từng loại tài sản công nghệ thông tin.

4. Căn cứ phân loại tài sản công nghệ thông tin tại khoản 1 Điều này, tổ chức xây dựng và thực hiện các quy định về quản lý và sử dụng tài sản theo quy định tại Điều 7, 8, 9, 10 và Điều 11 Thông tư này.

Điều 7. Quản lý tài sản thông tin

1. Với mỗi hệ thống thông tin phải lập danh sách tài sản thông tin, quy định về thẩm quyền, trách nhiệm của cá nhân hoặc bộ phận của tổ chức được tiếp cận,

khai thác và quản lý.

2. Tài sản thông tin phải phân loại theo quy định tại khoản 1 Điều 4 Thông tư này.

3. Tài sản thông tin thuộc loại thông tin bí mật phải được mã hóa hoặc có biện pháp bảo vệ để bảo mật thông tin trong quá trình tạo lập, trao đổi, lưu trữ.

4. Tài sản thông tin trên hệ thống thông tin mức độ 3 phải áp dụng phương án chống thất thoát dữ liệu.

Điều 8. Quản lý tài sản vật lý

1. Với mỗi hệ thống thông tin do tổ chức trực tiếp quản lý phải lập danh sách tài sản vật lý gồm các thông tin cơ bản sau: tên tài sản, giá trị, vị trí lắp đặt, chủ thể quản lý, mục đích sử dụng, tình trạng sử dụng, hệ thống thông tin tương ứng.

2. Tài sản vật lý phải được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.

3. Tài sản vật lý khi mang ra khỏi trụ sở của tổ chức phải được sự phê duyệt của cấp có thẩm quyền và phải thực hiện biện pháp bảo vệ để bảo mật thông tin lưu trữ trên tài sản nếu tài sản đó có chứa thông tin bí mật.

4. Tài sản vật lý có lưu trữ thông tin bí mật khi thay đổi mục đích sử dụng hoặc thanh lý phải được thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bí mật đó bảo đảm không có khả năng phục hồi. Trường hợp không thể tiêu hủy được thông tin bí mật, tổ chức thực hiện biện pháp tiêu hủy cấu phần lưu trữ dữ liệu trên tài sản đó.

5. Tài sản vật lý là thiết bị di động, vật mang tin, ngoài các quy định tại Điều này, phải được quản lý theo quy định tại Điều 10, Điều 11 Thông tư này.

Điều 9. Quản lý tài sản phần mềm

1. Với mỗi hệ thống thông tin phải lập danh sách tài sản phần mềm với các thông tin cơ bản gồm: tên tài sản, giá trị, mục đích sử dụng, phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin tương ứng.

2. Tài sản phần mềm phải được gán trách nhiệm cho cá nhân hoặc bộ phận quản lý.

3. Tài sản phần mềm phải được định kỳ rà soát và cập nhật các bản vá lỗi về an ninh bảo mật.

4. Tài sản phần mềm khi lưu trữ trên vật mang tin phải tuân thủ các quy định tại Điều 11 Thông tư này.

Điều 10. Quản lý sử dụng thiết bị di động

1. Các thiết bị di động khi kết nối vào hệ thống mạng nội bộ của tổ chức 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 tổ chức; kiểm soát các kết nối từ thiết bị di động tới các hệ thống thông tin được phép sử dụng tại tổ chức.

3. Quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.

4. Thiết bị di động được sử dụng để phục vụ công việc phải áp dụng các biện pháp kỹ thuật tối thiểu sau:

a) 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;

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

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

5. Với thiết bị di động là tài sản của tổ chức, ngoài việc áp dụng các quy định tại khoản 4 Điều này, phải áp dụng các biện pháp kỹ thuật tối thiểu sau đây:

a) 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;

b) Sử dụng các tính năng bảo vệ thông tin nội bộ, thông tin bí mật (nếu có); thiết lập mã khóa bí mật; cài đặt phần mềm phòng chống mã độc và các lỗi bảo mật khác.

Điều 11. Quản lý sử dụng vật mang tin

1. Kiểm soát việc đấu nối, gỡ bỏ vật mang tin với thiết bị thuộc hệ thống 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 thông tin bí mật chứa trong vật mang tin.

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

Mục 2
QUẢN LÝ NGUỒN NHÂN LỰC

Điều 12. Tổ chức nguồn nhân lực

1. Người đại diện hợp pháp phải trực tiếp tham gia chỉ đạo và có trách nhiệm

trong công tác xây dựng chiến lược, kế hoạch về bảo đảm an toàn thông tin, ứng cứu các sự cố an ninh mạng xảy ra tại tổ chức.

2. Tổ chức quản lý trực tiếp hệ thống thông tin mức độ 2 trở lên thực hiện:

a) Thành lập hoặc chỉ định bộ phận chuyên trách về an toàn thông tin có chức năng, nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an ninh mạng cho tổ chức;

b) Thành lập hoặc chỉ định bộ phận chuyên trách để quản lý vận hành trung tâm điều hành an ninh mạng đáp ứng yêu cầu quy định tại Điều 46 Thông tư này (không áp dụng với chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, tổ chức tín dụng phi ngân hàng);

c) Tách biệt nhân sự giữa các nhiệm vụ: (i) Phát triển với quản trị hệ thống thông tin; (ii) Phát triển với vận hành hệ thống thông tin; (iii) Quản trị với vận hành hệ thống thông tin; (iv) Kiểm tra về an toàn thông tin với phát triển, quản trị, vận hành hệ thống thông tin.

Điều 13. Tuyển dụng và phân công nhiệm vụ

Tổ chức tuyển dụng và phân công nhiệm vụ như sau:

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

2. Xem xét, đánh giá tư cách đạo đức, trình độ chuyên môn thông qua lý lịch, lý lịch tư pháp trước khi phân công nhân sự làm việc tại các vị trí quan trọng của hệ thống thông tin như: vận hành hệ thống thông tin mức độ 3 hoặc quản trị hệ thống thông tin.

3. Yêu cầu người được tuyển dụng 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 bảo đảm an toàn thông tin trong và sau khi làm việc tại tổ chức.

4. Đào tạo, phổ biến các quy định của tổ chức về an toàn thông tin đối với nhân sự mới tuyển dụng.

Điều 14. Quản lý sử dụng nguồn nhân lực

Tổ chức quản lý nguồn nhân lực như sau:

1. Phổ biến, cập nhật các quy định về an toàn thông tin cho tất cả cá nhân trong tổ chức tối thiểu mỗi năm một lần.

2. Kiểm tra việc tuân thủ các quy định về an toàn thông tin đối với cá nhân, bộ phận trực thuộc tối thiểu mỗi năm một lần.

3. Áp dụng các biện pháp xử lý kỷ luật đối với cá nhân, bộ phận vi phạm quy

định an toàn thông tin theo quy định của pháp luật và quy định của tổ chức.

Điều 15. Chấm dứt hoặc thay đổi công việc

Khi cá nhân trong tổ chức chấm dứt hoặc thay đổi công việc, tổ chức thực hiện:

1. Xác định trách nhiệm của cá nhân khi chấm dứt hoặc thay đổi công việc.

2. Yêu cầu cá nhân bàn giao lại tài sản công nghệ thông tin.

3. Thu hồi ngay quyền truy cập hệ thống thông tin của cá nhân nghỉ việc.

4. Thay đổi kịp thời quyền truy cập hệ thống thông tin của cá nhân thay đổi công việc bảo đảm nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao.

5. Rà soát, kiểm tra đối chiếu định kỳ tối thiểu sáu tháng một lần giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống thông tin nhằm bảo đảm tuân thủ khoản 3, khoản 4 Điều này.

6. Thông báo cho Ngân hàng Nhà nước (Cục Công nghệ thông tin) các trường hợp cá nhân làm việc trong lĩnh vực công nghệ thông tin của tổ chức 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 thông tin.

Mục 3
BẢO ĐẢM AN TOÀN VỀ MẶT VẬT LÝ VÀ MÔI TRƯỜNG NƠI LẮP ĐẶT TRANG THIẾT BỊ CÔNG NGHỆ THÔNG TIN

Điều 16. 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 17. Yêu cầu đối với trung tâm dữ liệu

Ngoài việc bảo đảm yêu cầu tại Điều 16 Thông tư này, Trung tâm dữ liệu phải bảo đảm các yêu cầu sau:

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

2. Cửa vào ra trung tâm dữ liệu phải chắc chắn, có khả năng chống cháy, sử dụng ít nhất hai loại khóa khác nhau và phải có biện pháp bảo vệ và giám sát 24/7.

3. Khu vực lắp đặt thiết bị phải được tránh nắng chiếu rọi trực tiếp, chống thấm dột nước, tránh ngập lụt. Khu vực lắp đặt thiết bị của hệ thống thông tin từ mức độ 2 trở lên 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. Nguồn điện phải đấu nối qua hệ thống lưu điện để cấp nguồn cho thiết bị, bảo đảm khả năng duy trì hoạt động liên tục của hệ thống thông tin.

5. Có hệ thống điều hòa không khí bảo đảm 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 bảo đảm 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; hệ thống tiếp địa.

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

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

11. Có hồ sơ nhật ký kiểm soát vào ra trung tâm dữ liệu.

Điều 18. An toàn 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 thông tin từ mức độ 2 trở lên 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 địa; có hệ thống máy phát điện dự phòng và hệ thống lưu điện bảo đảm 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. Các trang thiết bị dùng cho hoạt động nghiệp vụ lắp đặt bên ngoài trụ sở làm việc của tổ chức 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 19. Trách nhiệm quản lý và quy trình vận hành của tổ chức

1. Tổ chức ban hành các quy trình vận hành đối với hệ thống thông tin từ mức độ 2 trở lên, tối thiểu bao gồm: quy trình bật, tắt 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. Định kỳ tối thiểu mỗi năm một lần, tổ chức thực hiện rà soát, cập nhật, bổ sung các quy trình vận hành hệ thống thông tin để phù hợp thực tế.

2. Tổ chức triển khai các quy trình đến toàn bộ các đối tượng tham gia vận hành và giám sát tuân thủ việc thực hiện các quy trình đã ban hành.

3. Môi trường vận hành của hệ thống thông tin từ mức độ 2 trở lên phải đáp ứng yêu cầu:

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

b) Áp dụng các giải pháp bảo đảm an toàn thông tin;

c) Không cài đặt các công cụ, phương tiện phát triển ứng dụng;

d) Loại bỏ hoặc tắt các tính năng, phần mềm tiện ích không sử dụng trên hệ thống thông tin.

4. Đối với hệ thống thông tin xử lý giao dịch khách hàng phải đáp ứng yêu cầu sau:

a) Không để một cá nhân được đồng thời thực hiện các công việc khởi tạo và phê duyệt một giao dịch;

b) Áp dụng các biện pháp bảo đảm 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 20. Lập kế hoạch và chấp nhận hệ thống thông tin

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

2. Căn cứ các tiêu chuẩn, định mức, yêu cầu kỹ thuật đã xây dựng, tổ chức giám sát, tối ưu hiệu suất của hệ thống thông tin; đánh giá khả năng đáp ứng, tình trạng hoạt động, cấu hình hệ thống của hệ thống thông tin để dự báo, lập kế hoạch mở rộng, nâng cấp bảo đảm khả năng đáp ứng trong tương lai.

3. Tổ chức rà soát, cập nhật tiêu chuẩn, định mức, yêu cầu kỹ thuật khi có sự thay đổi đối với hệ thống 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 21. Sao lưu dự phòng

Tổ chức thực hiện sao lưu dự phòng bảo đảm an toàn dữ liệu như sau:

1. Lập danh sách hệ thống thông tin theo mức độ quan trọng cần được sao lưu, kèm theo thời gian lưu trữ, định kỳ sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.

2. Dữ liệu của các hệ thống thông tin từ mức độ 2 trở lên phải có phương án tự động sao lưu phù hợp với tần suất thay đổi của dữ liệu và bảo đảm nguyên tắc dữ liệu phát sinh phải được sao lưu trong vòng 24 giờ. Dữ liệu sao lưu phải được lưu trữ 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 lắp đặt hệ thống thông tin nguồn.

3. Đối với hệ thống thông tin từ mức độ 2 trở lên phải kiểm tra, phục hồi dữ liệu sao lưu từ phương tiện lưu trữ ngoài tối thiểu sáu tháng một lần.

4. Tổ chức có cả hệ thống thông tin chính và dự phòng đặt ngoài lãnh thổ Việt Nam phải thực hiện lưu trữ thông tin cá nhân, dữ liệu giao dịch của khách hàng tại Việt Nam theo quy định của pháp luật Việt Nam.

Điều 22. Quản lý an toàn, bảo mật hệ thống mạng

Tổ chức thực hiện quản lý an toàn, bảo mật hệ thống mạng như sau:

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

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

3. Xây dựng hệ thống mạng của tổ chức đáp ứng yêu cầu tối thiểu sau:

a) Chia tách thành các vùng mạng khác nhau theo đối tượng sử dụng, mục đích sử dụng và hệ thống thông tin, tối thiểu: (i) Có phân vùng mạng riêng cho máy chủ của hệ thống thông tin từ mức độ 2 trở lên; (ii) Có phân vùng mạng trung gian (DMZ) để cung cấp dịch vụ trên mạng Internet; (iii) Có phân vùng mạng riêng để cung cấp dịch vụ mạng không dây;

b) Có thiết bị có chức năng tường lửa để kiểm soát các kết nối, truy cập vào ra các vùng mạng quan trọng;

c) Có thiết bị có chức năng tường lửa và chức năng phát hiện phòng chống xâm nhập để kiểm soát kết nối, truy cập từ mạng không tin cậy vào hệ thống mạng

của tổ chức;

d) Có giải pháp kiểm soát, phát hiện và ngăn chặn kịp thời các kết nối, truy cập trái phép vào hệ thống mạng nội bộ của tổ chức có hệ thống thông tin từ mức độ 2 trở lên;

đ) Có phương án cân bằng tải và phương án ứng phó tấn công từ chối dịch vụ đối với các hệ thống thông tin từ mức độ 2 trở lên cung cấp dịch vụ trên mạng Internet.

4. Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị 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 23. Trao đổi thông tin

Trách nhiệm của tổ chức trong việc trao đổi thông tin với khách hàng và bên thứ ba:

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

2. Khi trao đổi thông tin nội bộ và thông tin bí mật với bên ngoài phải có văn bản thỏa thuận, xác định trách nhiệm và nghĩa vụ của các bên tham gia trong việc sử dụng, bảo đảm an toàn thông tin.

3. Các thông tin bí mật phải được mã hóa hoặc áp dụng các biện pháp bảo mật thông tin trước khi trao đổi.

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

5. 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.

Điều 24. Quản lý dịch vụ giao dịch trực tuyến

1. Yêu cầu đối với hệ thống thông tin của tổ chức thực hiện cung cấp dịch vụ giao dịch trực tuyến cho khách hàng:

a) Bảo đảm tính toàn vẹn của dữ liệu trao đổi với khách hàng trong giao dịch trực tuyến;

b) Dữ liệu trên đường truyền phải bảo đảm tính bí mật và phải được truyền đầy đủ, đúng địa chỉ và có biện pháp bảo vệ để tránh bị sửa đổi hoặc nhân bản trái phép;

c) Đánh giá mức độ rủi ro trong giao dịch trực tuyến theo đối tượng khách hàng, loại giao dịch, hạn mức giao dịch để cung cấp giải pháp xác thực giao dịch phù hợp theo quy định của Ngân hàng Nhà nước;

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

2. Xác thực giao dịch của khách hàng phải được thực hiện trực tiếp tại hệ thống thông tin của tổ chức. Trường hợp tổ chức sử dụng dịch vụ xác thực của bên thứ ba thì tổ chức phải quản lý tối thiểu một yếu tố xác thực.

3. Hệ thống dịch vụ giao dịch trực tuyến phải được áp dụng các biện pháp để giám sát chặt chẽ và phát hiện, cảnh báo về:

a) Giao dịch đáng ngờ dựa vào các tiêu chí tối thiểu gồm: thời gian giao dịch, địa điểm giao dịch (vị trí địa lý, địa chỉ IP mạng), tần suất giao dịch, số tiền giao dịch, số lần xác thực sai quy định;

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).

4. Tổ chức hướng dẫn các biện pháp bảo đảm an toàn thông tin và cảnh báo rủi ro cho khách hàng trước khi tham gia sử dụng dịch vụ giao dịch trực tuyến và theo định kỳ.

5. Khi cung cấp phần mềm ứng dụng giao dịch trực tuyến trên Internet phải áp dụng các biện pháp bảo đảm tính toàn vẹn của phần mềm.

Điều 25. Giám sát và ghi nhật ký hoạt động của hệ thống thông tin

Tổ chức thực hiện giám sát và ghi nhật ký hoạt động của hệ thống thông tin như sau:

1. Ghi và lưu trữ nhật ký về hoạt động của hệ thống thông tin và người sử dụng, các lỗi phát sinh, các sự cố an toàn thông tin. Dữ liệu nhật ký của các hệ thống thông tin từ mức độ 2 trở lên phải được lưu trữ trực tuyến tối thiểu 3 tháng theo hình thức tập trung và sao lưu tối thiểu một năm.

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

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

Điều 26. Phòng chống mã độc

Tổ chức xây dựng và thực hiện quy định về phòng chống mã độc như sau:

1. Xác định trách nhiệm của cá nhân 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 thông tin của tổ chức.

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 bảo đảm tuân thủ theo quy chế an toàn thông tin của tổ chức.

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

Mục 5
QUẢN LÝ TRUY CẬP

Điều 27. Yêu cầu đối với kiểm soát truy cập

1. Tổ chức 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 hệ thống thông tin bảo đảm đáp ứng yêu cầu nghiệp vụ và yêu cầu an toàn thông tin, 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) Mỗi tài khoản truy cập hệ thống phải được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung để truy cập hệ thống thông tin thì phải được phê duyệt bởi cấp có thẩm quyền và xác định được trách nhiệm cá nhân tại mỗi thời điểm sử dụng;

c) Đối với hệ thống thông tin từ mức độ 2 trở lên, phải giới hạn và kiểm soát các truy cập sử dụng tài khoản có quyền quản trị: (i) Thiết lập cơ chế kiểm soát việc tạo tài khoản có quyền quản trị để bảo đảm không một tài khoản nào sử dụng được khi chưa được cấp có thẩm quyền phê duyệt; (ii) Phải có biện pháp giám sát việc sử dụng tài khoản có quyền quản trị; (iii) Việc sử dụng tài khoản có quyền quản trị phải được giới hạn trong khoảng thời gian đủ để thực hiện công việc và phải được thu hồi ngay sau khi kết thúc công việc;

d) Quản lý, cấp phát mã khóa bí mật truy cập hệ thống thông tin;

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

e) Yêu cầu, điều kiện an toàn thông tin đối với các thiết bị, công cụ sử dụng để truy cập.

2. Tổ chức xây dựng quy định về quản lý mã khóa bí mật 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: (i) Yêu cầu thay đổi mã khóa bí mật lần đầu đăng nhập (không áp dụng với mã khóa bí mật sử dụng một lần); (ii) thông báo người sử dụng thay đổi mã khóa bí mật sắp hết hạn sử dụng; (iii) huỷ hiệu lực của mã khóa bí mật hết hạn sử dụng; (iv) hủy hiệu lực của mã khóa bí mật khi người sử dụng nhập sai quá số lần cho phép; (v) cho phép thay đổi ngay mã khóa bí mật bị lộ, có nguy cơ bị lộ hoặc theo yêu cầu của người sử dụng; (vi) ngăn chặn việc sử dụng lại mã khóa bí mật cũ trong một khoảng thời gian nhất định.

3. Tổ chức xây dựng quy định về trách nhiệm của người sử dụng khi được cấp quyền truy cập bao gồm các nội dung: 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; thoát khỏi hệ thống khi không làm việc hoặc tạm thời không làm việc trên hệ thống.

Điều 28. Quản lý truy cập mạng nội bộ

Tổ chức xây dựng và triển khai các chính sách quản lý truy cập mạng nội bộ đáp ứng các yêu cầu sau:

1. Xây dựng và triển khai 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 thông tin 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 mạng không tin cậy vào mạng nội bộ của tổ chức bảo đảm an toàn thông tin.

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 bảo đảm nguyên tắc quyền vừa đủ để thực hiện nhiệm vụ được giao.

6. Kết nối từ mạng Internet vào mạng nội bộ của tổ chức để phục vụ công việc phải sử dụng mạng riêng ảo và xác thực đa thành tố.

Điều 29. Quản lý truy cập hệ thống thông tin và ứng dụng

Tổ chức xây dựng và triển khai việc quản lý truy cập đáp ứng yêu cầu sau:

1. Kiểm soát những phần mềm tiện ích có khả năng ảnh hưởng đến hệ thống thông tin.

2. Quy định thời gian truy cập vào ứng dụng tương ứng với thời gian hoạt động nghiệp vụ và dịch vụ mà ứng dụng cung cấp. Tự động ngắt phiên làm việc của người sử dụng sau một thời gian không sử dụng nhằm ngăn chặn sự truy cập trái phép.

3. Quản lý và phân quyền truy cập thông tin và ứng dụng bảo đảm 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.

4. Các hệ thống thông tin sử dụng chung nguồn tài nguyên phải được cấp có thẩm quyền phê duyệt.

5. Đối với máy chủ thuộc hệ thống thông tin từ mức độ 2 trở lên phải sử dụng giao thức kết nối an toàn và có phương án chống đăng nhập tự động.

Điều 30. Quản lý kết nối Internet

Tổ chức quy định và triển khai việc quản lý kết nối Internet đáp ứng yêu cầu sau:

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 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 bảo đảm an toàn thông tin khi kết nối Internet.

2. Thực hiện quản lý tập trung, thống nhất các cổng kết nối Internet trong toàn bộ tổ chức.

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

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 tổ chức thông qua cổng kết nối Internet.

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

Điều 31. Các nguyên tắc chung về sử dụng dịch vụ của bên thứ ba

Khi sử dụng dịch vụ công nghệ thông tin của bên thứ ba, tổ chức bảo đảm các nguyên tắc sau đây:

1. Không làm suy giảm khả năng cung cấp dịch vụ liên tục của tổ chức cho khách hàng.

2. Không làm suy giảm việc kiểm soát quy trình nghiệp vụ của tổ chức.

3. Không làm thay đổi trách nhiệm của tổ chức trong việc bảo đảm an toàn thông tin.

4. Dịch vụ công nghệ thông tin của bên thứ ba phải đáp ứng các quy định về bảo đảm an toàn thông tin của tổ chức.

Điều 32. Các yêu cầu khi sử dụng dịch vụ của bên thứ ba

Trước khi sử dụng dịch vụ của bên thứ ba, tổ chức thực hiện:

1. Đánh giá rủi ro công nghệ thông tin, rủi ro hoạt động tối thiểu bao gồm các nội dung sau:

a) Nhận diện rủi ro, phân tích, ước lượng mức độ tổn hại, mối đe dọa đến an toàn thông tin;

b) Khả năng kiểm soát các quy trình nghiệp vụ, khả năng cung cấp dịch vụ liên tục cho khách hàng, khả năng thực hiện nghĩa vụ cung cấp thông tin cho các cơ quan nhà nước;

c) Xác định rõ vai trò, trách nhiệm của các bên liên quan trong việc bảo đảm chất lượng dịch vụ;

d) Xây dựng các biện pháp nhằm giảm thiểu rủi ro, biện pháp phòng ngừa, ứng cứu, khắc phục sự cố;

đ) Rà soát và điều chỉnh chính sách quản lý rủi ro (nếu có).

2. Trong trường hợp sử dụng dịch vụ điện toán đám mây, ngoài các yêu cầu tại khoản 1 Điều này, tổ chức thực hiện:

a) Phân loại hoạt động, nghiệp vụ dự kiến triển khai trên điện toán đám mây dựa trên đánh giá tác động của hoạt động, nghiệp vụ đó với hoạt động của tổ chức;

b) Xây dựng phương án dự phòng đối với các cấu phần của hệ thống thông tin từ mức độ 2 trở lên. Phương án dự phòng phải được kiểm thử và đánh giá sẵn sàng thay thế cho các hoạt động, nghiệp vụ triển khai trên điện toán đám mây;

c) Xây dựng các tiêu chí lựa chọn bên thứ ba đáp ứng yêu cầu quy định tại Điều 33 Thông tư này;

d) Rà soát, bổ sung, áp dụng các biện pháp bảo đảm an toàn thông tin của tổ chức, giới hạn truy cập từ điện toán đám mây đến các hệ thống thông tin của tổ chức.

3. Trường hợp thuê bên thứ ba thực hiện toàn bộ công việc quản trị hệ thống thông tin từ mức độ 2 trở lên, tổ chức thực hiện đánh giá rủi ro theo quy định tại khoản 1 Điều này và gửi báo cáo đánh giá rủi ro cho Ngân hàng Nhà nước (Cục Công nghệ thông tin).

Điều 33. Tiêu chí lựa chọn bên thứ ba cung cấp dịch vụ điện toán đám mây

Tiêu chí lựa chọn bên thứ ba bao gồm các nội dung tối thiểu sau:

1. Bên thứ ba phải là doanh nghiệp.

2. Có hạ tầng công nghệ thông tin tương ứng với dịch vụ mà tổ chức sử dụng đáp ứng các yêu cầu sau:

a) Các quy định của pháp luật Việt Nam;

b) Có chứng nhận quốc tế còn hiệu lực về bảo đảm an toàn thông tin.

Điều 34. Hợp đồng sử dụng dịch vụ với bên thứ ba

Hợp đồng sử dụng dịch vụ ký kết với bên thứ ba phải có tối thiểu những nội dung sau:

1. Cam kết của bên thứ ba về bảo đảm an toàn thông tin bao gồm:

a) Đáp ứng yêu cầu quy định tại Điều 33 Thông tư này;

b) Không sao chép, thay đổi, sử dụng hay cung cấp dữ liệu của tổ chức sử dụng dịch vụ cho cá nhân, tổ chức khác, trừ trường hợp có yêu cầu của cơ quan nhà nước có thẩm quyền theo quy định của pháp luật; trong trường hợp này, bên thứ ba phải thông báo cho tổ chức sử dụng dịch vụ trước khi cung cấp dữ liệu, trừ khi việc thông báo sẽ vi phạm pháp luật Việt Nam;

c) Phổ biến cho nhân sự của bên thứ ba tham gia thực hiện hợp đồng các quy định về bảo đảm an toàn thông tin của tổ chức, thực hiện các biện pháp giám sát bảo đảm tuân thủ.

2. Quy định cụ thể thời gian tối đa có thể gián đoạn dịch vụ và thời gian khắc phục sự cố, các yêu cầu liên quan đến bảo đảm hoạt động liên tục (dự phòng tại chỗ, sao lưu dữ liệu, dự phòng thảm họa), các yêu cầu liên quan đến năng lực xử lý, tính toán, lưu trữ, các biện pháp thực hiện khi chất lượng dịch vụ không được bảo đảm.

3. Trường hợp bên thứ ba sử dụng nhà thầu phụ không làm thay đổi trách nhiệm của bên thứ ba đối với dịch vụ mà tổ chức sử dụng.

4. Dữ liệu phát sinh trong quá trình sử dụng dịch vụ là tài sản của tổ chức. Khi chấm dứt sử dụng dịch vụ:

a) Bên thứ ba thực hiện trả lại toàn bộ dữ liệu triển khai và dữ liệu phát sinh trong quá trình sử dụng dịch vụ;

b) Bên thứ ba cam kết hoàn thành việc xoá toàn bộ dữ liệu của tổ chức trong một khoảng thời gian xác định.

5. Bên thứ ba phải thông báo cho tổ chức khi phát hiện nhân sự vi phạm quy định về an toàn thông tin đối với dịch vụ mà tổ chức sử dụng.

6. Hợp đồng sử dụng dịch vụ điện toán đám mây, ngoài các nội dung quy định tại các khoản 1, 2, 3, 4, 5 Điều này, phải bổ sung thêm những nội dung sau:

a) Bên thứ ba phải cung cấp báo cáo kiểm toán tuân thủ công nghệ thông tin do tổ chức kiểm toán độc lập thực hiện hàng năm trong thời gian thực hiện hợp đồng;

b) Bên thứ ba phải cung cấp: công cụ kiểm soát chất lượng dịch vụ đám mây; quy trình giám sát, kiểm soát chất lượng dịch vụ đám mây;

c) Bên thứ ba phải minh bạch các vị trí (thành phố, quốc gia) đặt trung tâm dữ liệu bên ngoài lãnh thổ Việt Nam triển khai dịch vụ cho tổ chức;

d) Trách nhiệm bảo vệ dữ liệu, chống truy cập dữ liệu trái phép trên kênh phân phối dịch vụ từ bên thứ ba đến tổ chức;

đ) Bên thứ ba phải hỗ trợ, hợp tác điều tra trong trường hợp có yêu cầu từ các cơ quan nhà nước có thẩm quyền của Việt Nam theo quy định của pháp luật;

e) Dữ liệu của tổ chức phải được tách biệt với dữ liệu của khách hàng khác sử dụng trên cùng nền tảng kỹ thuật do bên thứ ba cung cấp.

Điều 35. Trách nhiệm của tổ chức trong quá trình sử dụng dịch vụ của bên thứ ba

1. Cung cấp, thông báo và yêu cầu bên thứ ba thực hiện các quy định về an toàn thông tin của tổ chức.

2. Có quy trình và bố trí nguồn lực để giám sát, kiểm soát các dịch vụ do bên thứ ba cung cấp bảo đảm chất lượng dịch vụ theo thỏa thuận đã ký kết. Đối với dịch vụ điện toán đám mây, phải giám sát, kiểm soát chất lượng dịch vụ.

3. Áp dụng các quy định về an toàn thông tin của tổ chức đối với trang thiết bị, dịch vụ do bên thứ ba cung cấp được triển khai trên hạ tầng do tổ chức quản lý, sử dụng.

4. Quản lý các thay đổi đối với dịch vụ do bên thứ ba cung cấp bao gồm: thay đổi nhà cung cấp, thay đổi giải pháp, thay đổi phiên bản, thay đổi các nội dung quy định tại Điều 40 Thông tư này; đánh giá đầy đủ tác động của việc thay đổi, bảo đảm an toàn khi được đưa vào sử dụng.

5. Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép bên thứ ba truy cập vào hệ thống thông tin của tổ chức.

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

7. Thu hồi quyền truy cập hệ thống 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.

8. Đối với hệ thống thông tin từ mức độ 2 trở lên hoặc hệ thống thông tin sử dụng dịch vụ điện toán đám mây, phải đánh giá sự tuân thủ các quy định về bảo đảm an toàn thông tin của bên thứ ba theo đúng thỏa thuận đã ký kết. Thực hiện đánh giá sự tuân thủ định kỳ hàng năm hoặc đột xuất khi có nhu cầu. Việc đánh giá tuân thủ có thể sử dụng kết quả kiểm toán công nghệ thông tin của tổ chức kiểm toán độc lập.

Mục 7
QUẢN LÝ TIẾP NHẬN, PHÁT TRIỂN, DUY TRÌ HỆ THỐNG THÔNG TIN

Điều 36. Yêu cầu về an toàn, bảo mật các hệ thống thông tin

Khi xây dựng mới hoặc nâng cấp hệ thống thông tin do tổ chức quản lý trực tiếp, tổ chức phải thực hiện phân loại hệ thống thông tin theo mức độ quan trọng

quy định tại khoản 2 Điều 4 Thông tư này. Đối với hệ thống thông tin từ mức độ 2 trở lên, tổ chức thực hiện:

1. Xây dựng tài liệu thiết kế, mô tả về các phương án bảo đảm an toàn hệ thống thông tin. Trong đó các yêu cầu về an toàn, bảo mật được xây dựng đồng thời với việc xây dựng các yêu cầu kỹ thuật, nghiệp vụ.

2. Xây dựng phương án kiểm tra, xác minh hệ thống được triển khai tuân thủ theo đúng tài liệu thiết kế và yêu cầu bảo đảm an toàn thông tin trước khi nghiệm thu. Kết quả kiểm tra phải lập thành báo cáo và được cấp có thẩm quyền phê duyệt trước khi đưa vào vận hành chính thức.

3. Giám sát, quản lý chặt chẽ việc thuê mua phần mềm bên ngoài theo quy định tại Điều 35 Thông tư này.

Điều 37. Bảo đảm an toàn, bảo mật ứng dụng

Các chương trình ứng dụng nghiệp vụ phải đáp ứng các yêu cầu tối thiểu sau:

1. Kiểm tra tính hợp lệ của dữ liệu nhập vào các ứng dụng, bảo đảm 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 bảo đảm 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, bảo đảm 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 thông tin từ mức độ 2 trở lên phải được mã hóa ở lớp ứng dụng.

Điều 38. Quản lý mã hóa

Tổ chức quản lý mã hóa như sau:

1. Quy định và đưa vào sử dụng các biện pháp mã hóa theo quy chuẩn kỹ thuật quốc gia về mã hóa dữ liệu sử dụng trong lĩnh vực ngân hàng hoặc tiêu chuẩn quốc tế đã được công nhận.

2. Có biện pháp quản lý khóa mã hóa để bảo vệ thông tin của tổ chức.

Điều 39. An toàn, bảo mật trong quá trình phát triển phần mềm

1. Tổ chức thực hiện quản lý quá trình phát triển phần mềm như sau:

a) Quản lý, kiểm soát chương trình nguồn. Việc truy cập, tiếp cận chương trình nguồn phải được sự phê duyệt của cấp có thẩm quyền;

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

2. Tổ chức lựa chọn, kiểm soát đối với dữ liệu kiểm tra, thử nghiệm. Không sử dụng dữ liệu thật của hệ thống 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 chứa thông tin khách hàng và thông tin bí mật.

Điều 40. Quản lý sự thay đổi hệ thống thông tin

Tổ chức ban hành quy trình, biện pháp quản lý và kiểm soát sự thay đổi hệ thống thông tin, tối thiểu bao gồm:

1. Thực hiện ghi chép lại các thay đổi; lập kế hoạch thay đổi; thực hiện kiểm tra, thử nghiệm sự thay đổi, báo cáo kết quả; phê duyệt kế hoạch thay đổi trước khi áp dụng chính thức thay đổi phiên bản phần mềm, cấu hình phần cứng, tham số phần mềm hệ thống, quy trình vận hành. 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.

2. Kiểm tra, đánh giá tác động để bảo đảm hệ thống thông tin hoạt động ổn định, an toàn trên môi trường mới đối với hệ thống thông tin từ mức độ 2 trở lên khi thay đổi phiên bản hoặc thay đổi hệ điều hành, cơ sở dữ liệu, phần mềm lớp giữa.

Điều 41. Đánh giá an ninh bảo mật hệ thống thông tin

1. Nội dung đánh giá hệ thống thông tin của tổ chức về an ninh bảo mật phải bao gồm các nội dung 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) 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;

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

2. Tổ chức thực hiện đánh giá an ninh bảo mật đối với hệ thống thông tin từ mức độ 2 trở lên theo các nội dung quy định tại khoản 1 Điều này trước khi đưa vào vận hành chính thức.

3. Trong quá trình vận hành hệ thống thông tin, tổ chức định kỳ thực hiện đánh giá an ninh bảo mật tối thiểu như sau:

a) Sáu tháng một lần đối với hệ thống thông tin mức độ 3 theo các nội dung tại khoản 1 Điều này;

b) Một năm một lần đối với các hệ thống thông tin mức độ 2 và 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 khoản 1 Điều này;

c) Hai năm một lần đối với hệ thống thông tin mức độ 1.

4. Kết quả đánh giá phải được lập thành văn bản báo cáo người đại diện hợp pháp và cấp có thẩm quyền. Đối với các nội dung chưa tuân thủ quy định về an toàn thông tin (nếu có) phải đề xuất biện pháp, kế hoạch, thời hạn xử lý, khắc phục.

Điều 42. Quản lý các điểm yếu về mặt kỹ thuật

Tổ chức quản lý các điểm yếu về mặt kỹ thuật như sau:

1. Xây dựng quy định về việc đánh giá, quản lý và kiểm soát các điểm yếu về mặt kỹ thuật của các hệ thống thông tin đang sử dụng.

2. Chủ động phát hiện các điểm yếu về mặt kỹ thuật thông qua các hoạt động:

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 mã độc, lỗ hổng, điểm yếu về mặt kỹ thuật của các hệ thống thông tin đang sử dụng định kỳ tối thiểu như sau: (i) Ba tháng một lần đối với hệ thống thông tin mức độ 3 hoặc các hệ thống thông tin có kết nối với mạng Internet; (ii) Sáu tháng một lần đối với các hệ thống thông tin còn lại.

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

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

Điều 43. Quản lý bảo trì hệ thống thông tin

Tổ chức quản lý bảo trì hệ thống thông tin như sau:

1. Ban hành quy định bảo trì hệ thống thông tin ngay sau khi đưa vào hoạt động chính thức. Quy định bảo trì tối thiểu bao gồm các nội dung sau:

a) Phạm vi, các đối tượng được bảo trì;

b) Thời điểm, tần suất bảo trì;

c) Quy trình, kịch bản kỹ thuật để thực hiện bảo trì của từng cấu phần và toàn bộ hệ thống thông tin;

d) Khi thực hiện bảo trì nếu phát hiện, phát sinh sự cố phải báo cáo cấp có thẩm quyền để xử lý;

đ) Phân công và xác định trách nhiệm của bộ phận thực hiện bảo trì và giám sát bảo trì.

2. Thực hiện bảo trì theo quy định tại khoản 1 Điều này đối với hệ thống thông tin do tổ chức quản lý trực tiếp.

3. Rà soát quy định bảo trì tối thiểu một năm một lần hoặc khi hệ thống thông tin có sự thay đổi.

Mục 8
QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN

Điều 44. Quy trình xử lý sự cố

Tổ chức quản lý sự cố như sau:

1. Ban hành quy trình xử lý sự cố an toàn thông tin bao gồm những nội dung tối thiểu sau:

a) Tiếp nhận thông tin về sự cố phát sinh;

b) Đánh giá mức độ, phạm vi ảnh hưởng của sự cố đến hoạt động của hệ thống 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;

c) Thực hiện các biện pháp xử lý, khắc phục sự cố;

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

2. Quy định trách nhiệm của cá nhân, tập thể trong việc báo cáo, tiếp nhận, xử lý các sự cố an toàn thông tin.

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

Điều 45. Kiểm soát và khắc phục sự cố

Tổ chức kiểm soát và khắc phục sự cố như sau:

1. Lập danh sách sự cố an toàn thông tin và phương án xử lý sự cố đối với các hệ thống thông tin từ mức độ 2 trở lên; tối thiểu 6 tháng một lần thực hiện rà soát, cập nhật danh sách, phương án ứng cứu sự cố.

2. Lập tức báo cáo đến cấp có thẩm quyền và những người có liên quan khi phát sinh sự cố an toàn thông tin để có biện pháp khắc phục trong thời gian sớm nhất.

3. Trong quá trình kiểm tra, xử lý, khắc phục sự cố thu thập, ghi chép, bảo vệ chứng cứ và lưu trữ tại tổ chức.

4. Đánh giá xác định nguyên nhân và thực hiện các biện pháp phòng ngừa tránh sự cố tái diễn sau khi khắc phục sự cố.

5. Trong trường hợp sự cố an toàn thông tin có liên quan đến các vi phạm pháp luật, tổ chức có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

Điều 46. Trung tâm điều hành an ninh mạng

Trung tâm điều hành an ninh mạng thực hiện các nhiệm vụ sau:

1. Chủ động theo dõi, thu thập, tiếp nhận các thông tin, cảnh báo về các nguy cơ, rủi ro an toàn thông tin từ bên trong và bên ngoài.

2. Xây dựng hệ thống quản lý và phân tích sự kiện an toàn thông tin (SIEM), thực hiện thu thập và lưu trữ tập trung tối thiểu các thông tin: nhật ký của các hệ thống thông tin từ mức độ 2 trở lên; cảnh báo, nhật ký của trang thiết bị an ninh mạng (tường lửa, IPS/IDS).

3. Phân tích thông tin để phát hiện và cảnh báo về các rủi ro và các nguy cơ tấn công mạng, sự cố an ninh mạng và phải gửi cảnh báo đến người quản trị hệ thống khi phát hiện sự cố liên quan đến các hệ thống: (i) Hệ thống thông tin phục vụ khách hàng yêu cầu hoạt động 24/7; (ii) Hệ thống cung cấp giao dịch trực tuyến; (iii) Hệ thống thông tin mức độ 3.

4. Tổ chức điều phối ứng cứu sự cố và khoanh vùng, ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin khi sự cố phát sinh.

5. Điều tra, xác định nguồn gốc, cách thức, phương pháp tấn công và thực hiện các biện pháp phòng ngừa tránh sự số tái diễn.

6. Cung cấp thông tin theo yêu cầu của Ngân hàng Nhà nước để phục vụ giám sát an ninh mạng ngành Ngân hàng.

Điều 47. Hoạt động ứng cứu sự cố an ninh mạng

1. Mạng lưới ứng cứu sự cố an ninh mạng trong ngành Ngân hàng (Mạng lưới) có nhiệm vụ phối hợp các nguồn lực trong và ngoài ngành ứng phó hiệu quả sự cố an ninh mạng, góp phần bảo đảm hệ thống ngân hàng hoạt động an toàn.

2. Mạng lưới bao gồm:

a) Ban điều hành mạng lưới do Thống đốc Ngân hàng Nhà nước thành lập;

b) Cơ quan điều phối là Cục Công nghệ thông tin (Ngân hàng Nhà nước);

c) Các thành viên mạng lưới: Cục Công nghệ thông tin (Ngân hàng Nhà nước), tổ chức tín dụng (bộ phận chuyên trách an toàn thông tin) và thành viên tự nguyện tham gia mạng lưới là các cơ quan, tổ chức tự nguyện tham gia.

3. Nguyên tắc trong hoạt động điều phối và ứng cứu sự cố

a) Các tổ chức theo quy định tại điểm c khoản 2 Điều này phải có trách nhiệm cung cấp nguồn lực và tham gia làm thành viên mạng lưới;

b) Khi gặp sự cố an ninh mạng, các thành viên phải báo cáo Cơ quan điều phối theo quy định tại khoản 1 Điều 53 Thông tư này;

c) Khi gặp sự cố nghiêm trọng không tự khắc phục được, các thành viên phải gửi yêu cầu hỗ trợ đến Cơ quan điều phối;

d) Căn cứ vào từng sự cố, Cơ quan điều phối sẽ đề nghị các thành viên mạng lưới hỗ trợ hoặc các cơ quan nhà nước có thẩm quyền hỗ trợ, ứng cứu.

4. Nguyên tắc quản lý, sử dụng thông tin trong hoạt động điều phối và ứng cứu sự cố:

a) Thông tin được trao đổi, cung cấp trong quá trình điều phối và ứng cứu sự cố là thông tin bí mật;

b) Nghiêm cấm tổ chức, cá nhân sử dụng thông tin trao đổi trong quá trình điều phối và ứng cứu sự cố để làm ảnh hưởng đến uy tín, hình ảnh của tổ chức cung cấp thông tin.

Mục 9
BẢO ĐẢM HOẠT ĐỘNG LIÊN TỤC CỦA HỆ THỐNG THÔNG TIN

Điều 48. Nguyên tắc bảo đảm hoạt động liên tục

1. Tổ chức thực hiện các yêu cầu tối thiểu sau:

a) Phân tích tác động và đánh giá rủi ro đối với việc gián đoạn hoặc ngừng hoạt động của hệ thống thông tin;

b) Xây dựng quy trình và kịch bản bảo đảm hoạt động liên tục hệ thống thông tin theo quy định tại Điều 50 Thông tư này;

c) Tổ chức triển khai bảo đảm hoạt động liên tục theo quy định tại Điều 51 Thông tư này.

2. Trên cơ sở phân tích tác động và đánh giá rủi ro tại điểm a khoản 1 Điều này, tổ chức lập danh sách các hệ thống thông tin cần bảo đảm hoạt động liên tục tối thiểu bao gồm:

a) Hệ thống thông tin phục vụ hoạt động nội bộ hàng ngày của tổ chức và không chấp nhận ngừng vận hành quá 4 giờ làm việc;

b) Hệ thống phục vụ khách hàng yêu cầu hoạt động 24/7;

c) Hệ thống cung cấp giao dịch trực tuyến cho khách hàng;

d) Hệ thống thông tin mức độ 3.

3. Các hệ thống cần bảo đảm hoạt động liên tục tại Khoản 2 Điều này phải

bảo đảm tính sẵn sàng cao và có hệ thống dự phòng thảm họa.

Điều 49. Xây dựng hệ thống dự phòng thảm họa

1. Tổ chức xây dựng hệ thống dự phòng thảm họa đáp ứng các yêu cầu sau:

a) Đánh giá rủi ro và xem xét khả năng xảy ra các thảm họa ảnh hưởng đồng thời tới cả hệ thống thông tin chính và hệ thống thông tin dự phòng thảm họa khi lựa chọn địa điểm đặt hệ thống dự phòng thảm họa như: thảm họa tự nhiên như động đất, lũ lụt, bão, đại dịch; thảm họa do yếu tố con người và công nghệ như các sự cố về mạng lưới điện, hỏa hoạn, giao thông, tấn công an ninh mạng;

b) Địa điểm đặt hệ thống dự phòng phải đáp ứng các yêu cầu quy định tại Điều 16 Thông tư này;

c) Hệ thống dự phòng phải bảo đảm khả năng thay thế hệ thống chính trong khoảng thời gian: (i) 4 giờ đồng hồ đối với: hệ thống thông tin phục vụ hoạt động nội bộ hàng ngày của tổ chức và không chấp nhận ngừng vận hành quá 4 giờ làm việc, hệ thống phục vụ khách hàng yêu cầu hoạt động 24/7, hệ thống cung cấp giao dịch trực tuyến cho khách hàng, hệ thống thông tin mức độ 3; (ii) 24 giờ đồng hồ đối với các hệ thống khác.

2. Các tổ chức chỉ có một trụ sở làm việc tại Việt Nam phải có văn phòng dự phòng tại một địa điểm khác tách biệt trụ sở làm việc và có trang thiết bị để bảo đảm hoạt động liên tục thay thế trụ sở làm việc.

Điều 50. Xây dựng quy trình, kịch bản bảo đảm hoạt động liên tục

Tổ chức xây dựng quy trình, kịch bản bảo đảm hoạt động liên tục như sau:

1. Xây dựng quy trình xử lý các tình huống mất an toàn, gián đoạn hoạt động của từng cấu phần trong hệ thống thông tin từ mức độ 2 trở lên.

2. Xây dựng kịch bản chuyển đổi hệ thống dự phòng thay thế cho hoạt động của hệ thống chính, bao gồm nội dung công việc, trình tự thực hiện, dự kiến thời gian hoàn thành đáp ứng các nội dung sau:

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

b) Có các mẫu biểu ghi nhận kết quả;

c) 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, vận hành chính thức và kiểm tra kết quả;

d) Áp dụng biện pháp bảo đảm an toàn thông tin;

đ) Có phương án bảo đảm hoạt động liên tục khi việc chuyển đổi không thành công.

3. Các tổ chức chỉ có một trụ sở làm việc tại Việt Nam phải xây dựng kịch

bản chuyển đổi hoạt động sang văn phòng dự phòng.

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

Điều 51. Tổ chức triển khai bảo đảm hoạt động liên tục

1. Tổ chức phải có kế hoạch và tổ chức triển khai bảo đảm hoạt động liên tục hệ thống thông tin theo các yêu cầu sau:

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

b) Định kỳ hàng năm, thực hiện chuyển hoạt động chính thức từ hệ thống chính sang hệ thống dự phòng tối thiểu 1 ngày làm việc của từng hệ thống thông tin theo danh sách tại khoản 2 Điều 48 Thông tư này; đánh giá kết quả và cập nhật các quy trình, kịch bản chuyển đổi (nếu có).

2. Các tổ chức chỉ có một trụ sở làm việc tại Việt Nam phải tổ chức thực hiện diễn tập bảo đảm hoạt động liên tục định kỳ hàng năm.

3. Thông báo kế hoạch diễn tập chuyển đổi hoạt động liên tục cho Ngân hàng Nhà nước (Cục Công nghệ thông tin) chậm nhất là 5 ngày làm việc trước khi thực hiện.

Mục 10
KIỂM TRA NỘI BỘ VÀ CHẾ ĐỘ BÁO CÁO

Điều 52. Kiểm tra nội bộ

Tổ chức thực hiện kiểm tra nội bộ như sau:

1. Xây dựng quy định kiểm tra nội bộ về công tác bảo đảm an toàn thông tin của tổ chức.

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

3. Kết quả kiểm tra về công tác bảo đảm an toàn thông tin của tổ chức phải được lập thành báo cáo gửi người đại diện theo pháp luật và cấp có thẩm quyền, trong đó các vấn đề còn tồn tại chưa bảo đảm tuân thủ các quy định về an toàn thông tin (nếu có) phải có phương án xử lý, kế hoạch thực hiện.

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

Điều 53. Chế độ báo cáo

Tổ chức có trách nhiệm gửi báo cáo về Ngân hàng Nhà nước (Cục Công nghệ thông tin) các nội dung sau:

1. Báo cáo sự cố an ninh mạng trong vòng 24 giờ kể từ thời điểm sự cố được phát hiện và 05 ngày làm việc sau khi hoàn thành khắc phục sự cố theo Phụ lục kèm theo Thông tư này về địa chỉ thư điện tử antt@sbv.gov.vn.

2. Báo cáo đánh giá rủi ro theo quy định tại khoản 3 Điều 32 Thông tư này trực tiếp hoặc qua đường bưu điện về Ngân hàng Nhà nước (Cục Công nghệ thông tin, 64 Nguyễn Chí Thanh, Hà Nội) khi thuê ngoài toàn bộ công việc quản trị hệ thống thông tin từ mức độ 2 trở lên trước thời điểm triển khai tối thiểu 10 ngày làm việc.

Chương III
ĐIỀU KHOẢN THI HÀNH

Điều 54. Trách nhiệm của các đơn vị thuộc Ngân hàng Nhà nước

1. Cục Công nghệ thông tin có trách nhiệm:

a) Theo dõi, tổng hợp báo cáo Thống đốc Ngân hàng Nhà nước tình hình thực hiện của các tổ chức theo quy định tại Thông tư này;

b) Hàng năm lập kế hoạch kiểm tra việc thực hiện Thông tư này;

c) Chủ trì, phối hợp với các đơn vị liên quan thuộc Ngân hàng Nhà nước xử lý các vướng mắc phát sinh trong quá trình triển khai thực hiện Thông tư này.

2. Cơ quan Thanh tra, giám sát ngân hàng có trách nhiệm phối hợp với Cục Công nghệ thông tin kiểm tra việc thực hiện Thông tư này tại các tổ chức và xử lý vi phạm hành chính đối với hành vi vi phạm theo quy định của pháp luật.

Điều 55. Hiệu lực thi hành và tổ chức thực hiện

1. Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 01 năm 2019 trừ trường hợp quy định tại khoản 2 Điều này và thay thế Thông tư 31/2015/TT-NHNN ngày 28 tháng 12 năm 2015 của Thống đốc Ngân hàng Nhà nước ban hành Quy định về đảm bảo an toàn, bảo mật hệ thống công nghệ thông tin trong hoạt động ngân hàng và Quyết định 29/2008/QĐ-NHNN ngày 13 tháng 10 năm 2008 của Thống đốc Ngân hàng Nhà nước về việc ban hành Quy định về bảo trì hệ thống trang thiết bị tin học trong ngành Ngân hàng.

2. Điểm b khoản 2 Điều 12 có hiệu lực thi hành kể từ ngày 01 tháng 01 năm 2020.

3. Cục trưởng Cục Công nghệ thông tin, Thủ trưởng các đơn vị liên quan

thuộc Ngân hàng Nhà nước, 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 3 Điều 55;
- Ban Lãnh đạo NHNN;
- Văn phòng Chính phủ;
- Bộ Tư pháp (để kiểm tra);
- Công báo;
- Lưu VP, PC, CNTT (03 bản).

KT. THỐNG ĐỐC
PHÓ THỐNG ĐỐC

Nguyễn Kim Anh

Phụ lục

(Ban hành kèm theo Thông tư số ...../2018/TT-NHNN ngày ... tháng ... năm 2018)

TÊN TỔ CHỨC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**
Số: ...../.....	**Độc lập – Tự do – Hạnh phúc**

....., ngày tháng năm

BÁO CÁO SỰ CỐ AN NINH MẠNG

Mẫu 01 - Báo cáo ban đầu

Kính gửi: Cục Công nghệ thông tin - Ngân hàng Nhà nước

I. THÔNG TIN ĐẦU MỐI LIÊN HỆ

- Họ và tên: ..... Chức vụ: .....
- Đơn vị công tác:.....
- Địa chỉ: .....
- Điện thoại: ..... Email:.....

II. NỘI DUNG BÁO CÁO

1. Hệ thống thông tin gặp sự cố:.....

2. Mức độ quan trọng của hệ thống thông tin gặp sự cố:.....

3. Thời điểm phát hiện sự cố: ..... giờ.... phút ngày ...../...../.....

4. Mức độ ảnh hưởng ban đầu của sự cố:

- Hệ thống cung cấp dịch vụ cho khách hàng bị tác động ☐

  + Ảnh hưởng đến toàn bộ khách hàng ☐

  + Ảnh hưởng đến một số khách hàng ☐ ... / ... < *Số lượng khách hàng bị ảnh hưởng/Tổng khách hàng của Hệ thống thông tin*>

- Hệ thống thông tin nội bộ của đơn vị bị tác động ☐

  + Ảnh hưởng đến toàn bộ đơn vị ☐

  + Ảnh hưởng đến một số bộ phận ☐

- Các hệ thống thông tin liên quan bị ảnh hưởng:.....

- Mô tả chi tiết:

.....

.....

5. Loại sự cố (theo đánh giá ban đầu)

☐ Tấn công từ chối dịch vụ (DoS/DDoS) ☐ Virus/Worm/Trojan/Malware

☐ Xâm nhập/Tấn công/Truy cập trái phép ☐ Thay đổi giao diện web

☐ Sử dụng/khai thác hệ thống không phù hợp ☐ Tấn công Zero day/APT

☐ Tấn công Phishing/Social engineering

☐ Những sự cố khác (mô tả rõ):

.....

.....

6. Sự cố đã được báo cáo với VNCERT / bất kỳ cơ quan thực thi pháp luật nào chưa
(cung cấp rõ thời gian (ngày, giờ), tên cơ quan thực thi pháp luật đã được đơn vị báo cáo):

.....

III. KIẾN NGHỊ, ĐỀ XUẤT

.....

.....

.....

....., ngày .... tháng .... năm.....

Người đại diện hợp pháp
(ký, ghi rõ họ tên, đóng dấu)

TÊN TỔ CHỨC

Số: ...../.....

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

....., ngày tháng năm

BÁO CÁO SỰ CỐ AN NINH MẠNG

Mẫu 02 - Báo cáo hoàn thành khắc phục sự cố

Kính gửi: Cục Công nghệ thông tin - Ngân hàng Nhà nước

I. THÔNG TIN ĐẦU MỐI LIÊN HỆ

- Họ và tên: ..... Chức vụ: .....
- Đơn vị công tác:.....
- Địa chỉ: .....
- Điện thoại: ..... Email:.....

II. NỘI DUNG BÁO CÁO

1. Báo cáo cập nhật sự cố (điền đầy đủ thông tin bên dưới) ☐

+ Số văn bản báo cáo (trước đó) về sự cố: .....

+ Ngày báo cáo (trước đó): .....

2. Mức độ ảnh hưởng của sự cố:

- Hệ thống cung cấp dịch vụ cho khách hàng bị tác động ☐

+ Ảnh hưởng đến toàn bộ khách hàng ☐

+ Ảnh hưởng đến một số khách hàng ☐ ... / ... < *Số lượng khách hàng bị ảnh hưởng/Tổng khách hàng của Hệ thống thông tin*>.

- Hệ thống thông tin nội bộ của đơn vị bị tác động ☐

+ Ảnh hưởng đến toàn bộ đơn vị ☐

+ Ảnh hưởng đến một số bộ phận ☐

- Các hệ thống thông tin liên quan bị ảnh hưởng:.....

- Mô tả chi tiết:

.....

.....

3. Sự cố này có liên quan với những sự cố khác đã được báo cáo trước đó ?

☐ Không

☐ Có

- Cung cấp thông tin cụ thể hơn về sự cố trước đó:

.....

.....

.....

- Văn bản báo cáo liên quan đến sự cố đã được báo cáo trước đó: .....

4. Loại sự cố

☐ Tấn công từ chối dịch vụ (DoS/DDoS) ☐ Virus/Worm/Trojan/Malware

☐ Xâm nhập/Tấn công/Truy cập trái phép ☐ Thay đổi giao diện web

☐ Sử dụng/khai thác hệ thống không phù hợp ☐ Tấn công Zero day/APT

☐ Tấn công Phishing/Social engineering

☐ Những sự cố khác (mô tả rõ):

.....

.....

5. Thông tin về hệ thống gặp sự cố:

- Hệ điều hành ..... Version:.....

- Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

☐ Web server ☐ Mail server ☐ Database server

☐ Dịch vụ khác, đó là .....

- Cổng UDP hoặc TCP nào liên quan đến sự cố ☐ :.....

- Địa chỉ IP Public của những hệ thống bị ảnh hưởng ☐ :.....

- Địa chỉ IP tấn công ☐ : .....

6. Các biện pháp an toàn thông tin đã triển khai (trước khi hệ thống gặp sự cố)**:**

☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập

☐ Khác:

7. Sự cố đã được báo cáo với VNCERT / bất kỳ cơ quan thực thi pháp luật nào chưa
(cung cấp rõ thời gian (ngày, giờ), tên cơ quan thực thi pháp luật đã được đơn vị báo cáo)**:**

.....

8. Các hoạt động bảo lưu bằng chứng có được triển khai:

.....

9. Các hoạt động ngăn ngừa, cô lập sự cố có được triển khai:

.....

10. Phương án khắc phục sự cố

(Cung cấp thông tin chi tiết về sự cố: tóm tắt nguyên nhân; các biện pháp đã thực hiện để ngăn chặn, khắc phục và phòng ngừa; thiệt hại liên quan đến sự cố).

.....

III. KIẾN NGHỊ, ĐỀ XUẤT

.....

.....

....., ngày .... tháng .... năm.....

Người đại diện hợp pháp

(ký, ghi rõ họ tên, đóng dấu)