NGÂN HÀNG NHÀ NƯỚC VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 09 /2020/TT-NHNN	*Hà Nội, ngày 21 tháng 10 năm 2020*

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 Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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 những yêu cầu tối thiểu 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, chi nhánh ngân hàng nước ngoài, các tổ chức cung ứng dịch vụ trung gian thanh toán, công ty thông tin tín dụng, Công ty Cổ phần Thanh toán Quốc gia Việt Nam, Công ty Quản lý tài sản của các tổ chức tín dụng Việt Nam, Nhà máy in tiền quốc gia, Bảo hiểm tiền gửi Việt Nam (sau đây gọi chung là tổ chức) có thiết lập và sử dụng hệ thống thông tin phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của tổ chức.

Điều 2. Giải thích từ ngữ

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

1. 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.

2. Sự cố an toàn thông tin là việc thông tin số, hệ thống thông tin bị tấn công hoặc bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng của thông tin.

3. 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.

4. 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.

5. 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.

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

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

8. 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.

9. Dịch vụ điện toán đám mây là các dịch vụ cung cấp tài nguyên máy tính (bao gồm tài nguyên tính toán, tài nguyên kết nối mạng, tài nguyên lưu trữ, tài nguyên phần mềm và các tài nguyên máy tính khác) qua môi trường mạng cho phép nhiều đối tượng sử dụng, có thể điều chỉnh và thanh toán theo nhu cầu sử dụng.

10. 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.

11. 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.

12. Người đại diện hợp pháp của tổ chức là người đại diện theo pháp luật của tổ chức tín dụng, doanh nghiệp, Tổng giám đốc (Giám đốc) chi nhánh ngân hàng nước ngoài.

13. 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.

14. Xác thực đa yếu tố là phương pháp xác thực yêu cầu tối thiểu hai yếu tố để chứng minh tính đúng đắn của một danh tính. Các yếu tố xác thực bao gồm: (i) Những thông tin mà người dùng biết (số PIN, mã khoá bí mật, ...); (ii) Những gì mà người dùng sở hữu (thẻ thông minh, thiết bị token, điện thoại di động ...); (iii) Những dấu hiệu sinh trắc học của người dùng.

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. Hệ thống thông tin được phân loại theo cấp độ quy định tại Điều 5 Thông tư này và áp dụng chính sách an toàn thông tin phù hợp.

3. Các rủi ro công nghệ thông tin có thể xảy ra trong tổ chức được nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả.

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

Điều 4. Phân loại thông tin

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

1. 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;

2. Thông tin riêng (hoặc thông tin nội bộ) là thông tin được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng được xác định danh tính;

3. Thông tin cá nhân là thông tin định danh khách hàng và các thông tin sau đây: thông tin về tài khoản, thông tin về tiền gửi, thông tin về tài sản gửi, thông tin về giao dịch và các thông tin có liên quan khác;

4. Thông tin bí mật là: (i) Thông tin Mật, Tối Mật, Tuyệt Mật theo quy định

của pháp luật về bảo vệ bí mật nhà nước; (ii) Thông tin hạn chế tiếp cận theo quy định của tổ chức.

Điều 5. Phân loại hệ thống thông tin

1. Đối với hệ thống thông tin cung cấp dịch vụ trực tuyến cho khách hàng, các tổ chức thực hiện phân loại theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ. Đối với các hệ thống thông tin khác, thực hiện phân loại theo quy định tại khoản 2, 3, 4, 5, 6, 7 Điều này.

2. Hệ thống thông tin cấp độ 1 là hệ thống thông tin phục vụ hoạt động nội bộ của tổ chức và chỉ xử lý thông tin công cộng.

3. Hệ thống thông tin cấp độ 2 là hệ thống thông tin có một trong các tiêu chí sau:

a) Hệ thống thông tin phục vụ hoạt động nội bộ của tổ chức, có xử lý thông tin riêng, thông tin cá nhân của người sử dụng, thông tin hạn chế tiếp cận theo quy định của tổ chức nhưng không xử lý thông tin bí mật nhà nước;

b) Hệ thống thông tin phục vụ khách hàng không yêu cầu vận hành 24/7;

c) Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của một số bộ phận thuộc tổ chức hoặc của tổ chức tài chính vi mô, quỹ tín dụng nhân dân cơ sở.

4. Hệ thống thông tin cấp độ 3 là hệ thống thông tin có một trong các tiêu chí sau:

a) Hệ thống thông tin xử lý thông tin bí mật nhà nước ở cấp độ Mật;

b) 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 kể từ thời điểm ngừng vận hành;

c) 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;

d) Các hệ thống thanh toán sử dụng của bên thứ ba dùng để thanh toán ngoài hệ thống của tổ chức;

đ) Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của tổ chức và của ngành Ngân hàng.

5. Hệ thống thông tin cấp độ 4 là hệ thống thông tin có một trong các tiêu chí sau:

a) Hệ thống thông tin xử lý thông tin bí mật nhà nước ở cấp độ Tối Mật;

b) Hệ thống thông tin phục vụ khách hàng có xử lý, lưu trữ dữ liệu của 10 triệu khách hàng trở lên;

c) Hệ thống thông tin quốc gia trong ngành Ngân hàng, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước;

d) Các hệ thống thanh toán quan trọng trong ngành Ngân hàng theo quy định của Ngân hàng Nhà nước;

đ) Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của ngành Ngân hàng, yêu cầu vận hành 24/7 và không chấp nhận ngừng vận hành mà không có kế hoạch trước.

6. Hệ thống thông tin cấp độ 5 là hệ thống thông tin có một trong các tiêu chí sau:

a) Hệ thống thông tin xử lý thông tin bí mật nhà nước ở cấp độ Tuyệt Mật;

b) Hệ thống thông tin quốc gia trong ngành Ngân hàng phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế;

c) Hệ thống cơ sở hạ tầng thông tin quốc gia trong ngành Ngân hàng phục vụ kết nối liên thông hoạt động của Việt Nam với quốc tế.

7. Trong trường hợp hệ thống thông tin bao gồm nhiều hệ thống thành phần, mỗi hệ thống thành phần lại tương ứng với một cấp độ khác nhau, cấp độ hệ thống thông tin được xác định là cấp độ cao nhất trong các cấp độ của các hệ thống thành phần cấu thành.

8. Tổ chức thực hiện phân loại hệ thống thông tin theo cấp độ quy định tại khoản 1, 2, 3, 4, 5, 6, 7 Điều này. Hồ sơ, thủ tục thẩm định, phê duyệt hệ thống thông tin theo cấp độ tuân thủ quy định tại Nghị định số 85/2016/NĐ-CP. Đối với hồ sơ đề xuất các hệ thống thông tin cấp độ 4, 5, tổ chức gửi hồ sơ cho Ngân hàng Nhà nước (Cục Công nghệ thông tin) để lấy ý kiến.

9. Danh sách hệ thống thông tin theo cấp độ phải được lập và rà soát, cập nhật sau khi hệ thống được triển khai và định kỳ hàng năm.

Điều 6. 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;