TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

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

08:12 02/09/2018

Ngân hàng Nhà nước đã ban hành Thông tư quy định về an toàn hệ thống thông tin trong hoạt động ngân hàng nhằm cập nhật các quy định mới của Luật An toàn thông tin mạng.

Ngày 21/8/2018, Thống đốc Ngân hàng Nhà nước đã ký ban hành Thông tư số 18/2018/TT-NHNN thay thế Thông tư 31/2015/TT-NHNN ngày 28/12/2015 quy định về đảm bảo an toàn, bảo mật hệ thống CNTT trong hoạt động ngân hàng. Thông tư này có hiệu lực thi hành từ 1/1/2019.

Thông tư được ban hành nhằm cập nhật các quy định mới của Luật An toàn thông tin mạng và các văn bản hướng dẫn, đồng thời điều chỉnh các yêu cầu về an ninh bảo mật phù hợp với thực tế phát triển nhanh chóng, đa dạng của CNTT và tình hình an toàn thông tin mạng trong ngành Ngân hàng.



Ảnh minh họa

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

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.

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.

Quy chế an toàn thông tin tối thiểu gồm các nội dung cơ bản sau: Quản lý tài sản công nghệ thông tin; quản lý nguồn nhân lực; bảo đảm an toàn về mặt vật lý và môi trường lắp đặt; quản lý vận hành và trao đổi thông tin; quản lý truy cập; quản lý sử dụng dịch vụ công nghệ thông tin của bên thứ ba; quản lý tiếp nhận, phát triển, duy trì hệ thống thông tin; quản lý sự cố an toàn thông tin; bảo đảm hoạt động liên tục của hệ thống thông tin.

Yêu cầu đối với hệ thống thông tin của tổ chức thực hiện cung cấp dịch vụ giao dịch trực tuyến cho khách hàng: Bảo đảm tính toàn vẹn của dữ liệu trao đổi với khách hàng trong giao dịch trực tuyến; 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; 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.

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.

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: 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.

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

Thông tư này có hiệu lực thi hành từ 1-1-2019.

Diệp Bắc