|  |  |
| --- | --- |
| NGÂN HÀNG NHÀ NƯỚCVIỆT NAM**CỤC CÔNG NGHỆ THÔNG TIN** | CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆTNAM**Độc lập - Tự do - Hạnh phúc**Hà Nội, ngày tháng năm 2020 |

**BẢN THUYẾT MINH DỰ THẢO**

**Thông tư thay thế Thông tư 18/2018/TT-NHNN**

1. **Sự cần thiết phải ban hành Thông tư thay thế Thông tư 18/2018/TT-NHNN**

Thông tư 18/2018/TT-NHNN ngày 21/08/2018 của Thống đốc Ngân hàng Nhà nước được ban hành đã tạo hành lang pháp lý và hướng dẫn toàn diện cho các tổ chức tín dụng, tổ chức trung gian thanh toán và một số tổ chức khác trong công tác đảm bảo an toàn thông tin. Nhằm cập nhật đầy đủ các quy định của Luật An toàn thông tin mạng và các văn bản hướng dẫn đồng thời phù hợp với thực tế tình hình an toàn thông tin mạng trong ngành Ngân hàng, Ngân hàng Nhà nước Việt Nam (Cục Công nghệ thông tin) đã nghiên cứu, hoàn thành Dự thảo Thông tư thay thế Thông tư 18/2018/TT-NHNN (sau đây gọi là Dự thảo Thông tư).

1. ***Cơ sở pháp lý***

Ngày 19/11/2015, Quốc hội đã thông qua Luật An toàn thông tin mạng số 86/2015/QH13. Trên cơ sở các quy định của Luật, Chính phủ đã ban hành Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ. Bộ Thông tin và truyền thông đã ban hành Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP; Tiêu chuẩn TCVN 11930:2017 về Các yêu cầu kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

Ngày 11/6/2019 Chính phủ đã ban hành Nghị quyết 08/NQ-CP về việc ban hành chương trình hành động thực hiện Nghị quyết số 29-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược bảo vệ Tổ quốc trên không gian mạng. Trong đó có nội dung chỉ đạo các Bộ Ngành nghiên cứu, rà soát, sửa đổi, bổ sung, hoàn thiện văn bản quy phạm pháp luật về an toàn thông tin mạng.

Triển khai Quyết định số 2756/QĐ-NHNN ngày 31/12/2020 của Thống đốc Ngân hàng Nhà nước về việc ban hành chương trình xây dựng Thông tư năm 2020 của Ngân hàng Nhà nước Việt Nam.

1. ***Cơ sở thực tiễn***

Trong năm 2019 và nửa đầu năm 2020, theo thông tin từ Bộ Công an, Bộ Thông tin và Truyền thông và qua công tác giám sát về an ninh mạng của ngành Ngân hàng, các cuộc tấn công mạng nhằm vào hệ thống ngân hàng gia tăng cả về quy mô và mức độ dai dẳng lẫn thủ đoạn tinh vi. Cuối 2019, ngành Ngân hàng Việt Nam đã xảy ra vụ việc liên quan đến công tác đảm bảo an toàn thông tin như lộ lọt thông tin khách hàng, phát hiện mã độc tấn công xâm nhập vào hệ thống thông tin.

Qua công tác kiểm tra và khảo sát, Cục CNTT đã ghi nhận được các khó khăn, vướng mắc và các đề xuất trong quá trình triển khai thực hiện Thông tư 18/2018/TT-NHNN của các tổ chức tín dụng, tổ chức cung ứng dịch vụ trung gian thanh toán.

Dự thảo Thông tư thay thế để giải quyết vấn đề nảy sinh trong hoạt động CNTT tại các tổ chức, cụ thể với quy định về phân loại hệ thống thông tin theo ba mức độ, do số lượng các hệ thống thông tin nhiều, tập trung vào mức độ 2 (hệ thống thông tin quan trọng) nên các tổ chức gặp nhiều khó khăn, vướng mắc trong đầu tư nguồn lực để quản lý an toàn các hệ thống thông tin.

1. **Nguyên tắc, định hướng xây dựng Dự thảo Thông tư**
* Thông tư 18/2018/TT-NHNN được xây dựng dựa trên phương pháp luận lấy hệ thống CNTT làm đối tượng chính, điều chỉnh mọi hoạt động, tương tác liên quan trong toàn bộ vòng đời hệ thống CNTT, Dự thảo Thông tư vẫn theo nguyên tắc và bố cục như vậy.
* Triển khai Luật An toàn thông tin mạng, Dự thảo Thông tư cập nhật quy định phân loại hệ thống thông tin theo cấp độ trên cơ sở các quy định tại Nghị định 85/2016/NĐ-CP, Thông tư 03/2017/TT-BTTTT, Tiêu chuẩn TCVN 11930:2017 và có những hướng dẫn để phù hợp với đặc thù của ngành Ngân hàng.
* Cập nhật quy định phân loại thông tin, hệ thống thông tin và quy định liên quan đến đảm bảo an toàn, an ninh cho từng cấp độ hệ thống thông tin nhằm đảm bảo tính khả thi và hài hòa về đầu tư nguồn lực cho yêu cầu an toàn bảo mật với từng cấp độ hệ thống thông tin.

Các quy định được sửa đổi, bổ sung, loại bỏ được nêu chi tiết trong Phụ lục 01 – Bảng so sánh Thông tư 18/2018/TT-NHNN và Dự thảo Thông tư (đính kèm).

1. **Các nội dung chính cần lấy ý kiến**
2. **Bổ sung đối tượng điều chỉnh**

Bổ sung một số đối tượng áp dụng thuộc phạm vi quản lý, cấp phép của NHNN hiện chưa có các quy định về tuân thủ bảo đảm an toàn hệ thống thông tin như: công ty thông tin tín dụng (hiện có Công ty Cổ phần thông tin tín dụng Việt Nam – PCB), Công ty Quản lý tài sản của các tổ chức tín dụng Việt Nam (VAMC), Nhà máy in tiền quốc gia, Bảo hiểm tiền gửi Việt Nam.

Bổ sung đối tượng Tổ chức tài chính vi mô, Quỹ tín dụng nhân dân cơ sở trong trường hợp các tổ chức này 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.

1. **Phân loại hệ thống thông tin theo 5 cấp độ**

Dự thảo Thông tư quy định đối với các hệ thống cung cấp dịch vụ trực tuyến cho khách hàng phải tuân thủ phân loại hệ thống theo quy định tại Nghị định 85/2016/NĐ-CP và các văn bản hướng dẫn.

Đối với các hệ thống khác, thực hiện phân loại theo 5 cấp độ trên cơ sở tham khảo quy định tại Nghị định 85/2016/NĐ-CP và phù hợp với đặc thù ngành Ngân hàng, thay thế phân loại 3 mức độ theo quy định tại Thông tư 18/2018/TT-NHNN có một số bất cập gây khó khăn cho các tổ chức khi triển khai thực hiện.

1. **Tần suất của các hoạt động sao lưu dữ liệu, dò quét điểm yếu, đánh giá an ninh bảo mật**

Trên cơ sở các hệ thống thông tin được phân loại theo cấp độ, các yêu cầu về an toàn bảo mật với từng hệ thống thông tin theo cấp độ có sự khác nhau, dẫn đến nguồn lực cần triển khai cũng khác nhau như:

* Tần suất sao lưu và phục hồi dữ liệu;
* Tần suất thực hiện dò quét điểm yếu và đánh giá an ninh bảo mật;

Các nội dung nêu trên là những vấn đề quan trọng có ảnh hưởng đến nguồn lực của các tổ chức khi đầu tư cho an toàn thông tin nên cần được xem xét thận trọng, cân bằng giữa lợi ích và rủi ro đối với từng HTTT theo cấp độ.

1. **Triển khai áp dụng các giải pháp xác thực đa thành tố trong quản trị và vận hành các hệ thống thông tin**
* Áp dụng xác thực đa thành tố khi phê duyệt giao dịch tài chính phát sinh chuyển tiền điện tử sang đối tác bên ngoài có giá trị từ 100 triệu trở lên;
* Đối với các hệ thống thông tin từ cấp độ 4 trở lên phải áp dụng xác thực đa thành tố đối với các tài khoản quản trị máy chủ, ứng dụng và các thiết bị mạng, an ninh mạng quan trọng.

**CỤC CÔNG NGHỆ THÔNG TIN**