|  |  |
| --- | --- |
| NGÂN HÀNG NHÀ NƯỚC  VIỆT NAM  **CỤC CÔNG NGHỆ THÔNG TIN** | CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆTNAM  **Độc lập - Tự do - Hạnh phúc** Hà Nội, ngày tháng 4 năm 2018 |

**BẢN THUYẾT MINH DỰ THẢO**

**Thông tư thay thế Thông tư 31/2015/TT-NHNN**

1. **Sự cần thiết phải ban hành Thông tư thay thế Thông tư 31/2015/TT-NHNN**

Thông tư 31/2015/TT-NHNN ngày 28/12/2015 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 trong công tác đảm bảo an toàn thông tin. Nhằm cập nhật các quy định mới của Luật An toàn thông tin mạng và các văn bản hướng dẫn đồng thời phản ánh đầy đủ, sát thực hơn các yêu cầu về an ninh bảo mật phù hợp với thực tế phát triển nhanh chóng, đa dạng về công nghệ thông tin (CNTT) và 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 31/2015/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 ban hành các văn bản hướng dẫn thi hành Luật An toàn thông tin mạng.

Triển khai Chỉ thị số 01/CT-NHNN ngày 10/01/2018 của Thống đốc Ngân hàng Nhà nước về việc Tổ chức triển khai các nhiệm vụ, giải pháp trọng tâm của Ngành ngân hàng 2018 nhiệm vụ 4.2 “…*Rà soát, cập nhật các văn bản quy phạm pháp luật về an ninh, an toàn, bảo mật thông tin liên quan tới thanh toán điện tử, thanh toán thẻ phù hợp với diễn biến phát triển, ứng dụng công nghệ, thực trạng tội phạm mạng trong lĩnh vực ngân hàng*”.

1. ***Cơ sở thực tiễn***

Dự thảo Thông tư sửa đổi để đáp ứng một số vấn đề nảy sinh trong hoạt động CNTT như:

* Xu hướng phát triển CNTT có nhiều thay đổi, vài năm gần đây đã xuất hiện loại hình thuê ngoài dịch vụ CNTT, trong đó các dịch vụ CNTT có thể thuê bên thứ 3 cung cấp quản lý, vận hành.
* Dịch vụ điện toán đám mây có đặc điểm là cơ sở hạ tầng CNTT cũng như dữ liệu của khách hàng sử dụng dịch vụ có thể được xử lý bên ngoài lãnh thổ Việt Nam. Điều này đặt ra vấn đề về bảo đảm chủ quyền đối với dữ liệu, đảm bảo hoạt động liên tục với các dịch vụ tài chính ngân hàng triển khai trên nền tảng điện toán đám mây và quyền tiếp cận thông tin của Cơ quan quản lý Nhà nước Việt Nam. Để tạo điều kiện cho các tổ chức tín dụng sử dụng các dịch vụ điện toán đám mây hiệu quả và an toàn, Dự thảo Thông tư quy định các nội dung về lựa chọn, triển khai các dịch vụ tài chính trên nền tảng điện toán đám mây đảm bảo an toàn và bảo mật.
* Ngoài ra, trên cơ sở khảo sát các khó khăn, vướng mắc và các đề xuất của các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức trung gian thanh toán trong quá trình triển khai thực hiện Thông tư 31/2015/TT-NHNN Dự thảo Thông tư cũng có một số điều chỉnh để phù hợp với hoạt động thực tiễn.

1. **Nguyên tắc, định hướng xây dựng Dự thảo Thông tư**

* Thông tư 31/2015/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 bổ sung quy định mới về phân loại hệ thống thông tin theo cấp độ trên cơ sở tham khảo các quy định tại Nghị định 85/2016/NĐ-CP và Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP với những điều chỉnh để phù hợp với đặc thù của ngành Ngân hàng.
* Rà soát, hợp nhất nội dung tại Quyết định số 29/2008/QĐ-NHNN của Thống đốc Ngân hàng Nhà nước về bảo trì hệ thống trang thiết bị tin học trong ngành Ngân hàng.
* Sửa đổi, bổ sung quy định về sử dụng dịch vụ CNTT của bên thứ 3; bổ sung thêm các nội dung để phù hợp với đặc điểm “dịch vụ điện toán đám mây”.
* Bổ sung quy định về hoạt động ứng cứu sự cố ngành Ngân hàng và trung tâm điều hành an ninh mạng (SOC), tạo cơ sở pháp lý và nâng cao hiệu quả hoạt động của mạng lưới ứng cứu sự cố an toàn thông tin và hoạt động giám sát an ninh mạng trong ngành Ngân hàng nhằm theo dõi, giám sát phát hiện sớm các nguy cơ tấn công và thu thập thông tin để điều tra sự cố.

Các quy định được sửa đổi, bổ sung, loại bỏ được nêu chi tiết trong Phụ lục 01 – Bảng so sánh Thông tư 31/2015/TT-NHNN và Dự thảo Thông tư (đính kèm).

1. **Các nội dung chính cần lấy ý kiến**
2. **Phân loại hệ thống thông tin theo 5 cấp độ**

Dự thảo Thông tư đã tham khảo Nghị định 85/2016/NĐ-CP để phân loại hệ thống thông tin theo 5 cấp độ phù hợp với ngành Ngân hàng. Mục đích của việc phân loại hệ thống thông tin theo cấp độ nhằm đưa ra các quy định quản lý an toàn, bảo mật phù hợp với mức độ rủi ro theo từng cấp độ của hệ thống thông tin.

1. **Quản lý sử dụng dịch vụ CNTT của bên thứ ba**

Bên cạnh những lợi ích mà dịch vụ điện toán đám mây mang lại vẫn còn tồn tại một số vấn đề như:

* Khó khăn trong việc kiểm soát, bảo đảm an toàn thông tin mạng, bảo vệ dữ liệu. Tăng nguy cơ bị tấn công mạng, tăng nguy cơ lộ, lọt thông tin/dữ liệu mật;
* Gián đoạn trong việc cung cấp dịch vụ do các sự cố liên quan đến kết nối mạng;
* Chủ quyền đối với dữ liệu và quyền tiếp cận thông tin của đơn vị sử dụng dịch vụ và Cơ quan quản lý Nhà nước Việt Nam có thể có xung đột với nhà cung cấp dịch vụ trong trường hợp có sự khác biệt về mặt pháp lý giữa quốc gia mà đơn vị cung cấp dịch vụ được cấp phép thành lập với pháp lý của Nhà nước Việt Nam.

Với những rủi ro như vậy, các quy định tại “Mục 6. Quản lý dịch vụ CNTT của bên thứ ba” được xây dựng với quan điểm tạo cơ hội tiếp cận dịch vụ điện toán đám mây cho các đơn vị trong ngành Ngân hàng nhằm giúp tiết giảm chi phí đầu tư hạ tầng CNTT và chi phí nâng cao chất lượng nguồn nhân lực, tinh gọn cơ cấu tổ chức, nhưng vẫn đảm bảo an toàn, an ninh. Theo đó:

* Việc sử dụng dịch vụ điện toán đám mây cần phù hợp với mức độ rủi ro của từng cấp độ hệ thống thông tin. Đảm bảo hoạt động liên tục, giảm thiểu các rủi ro liên quan đến gián đoạn kết nối mạng;
* Đảm bảo chủ quyền đối với dữ liệu của đơn vị sử dụng dịch vụ và hiệu lực thực thi pháp luật của Cơ quan Nhà nước Việt Nam trong việc tiếp cận thông tin;
* Giảm thiểu sự phụ thuộc vào bên thứ 3 và đảm bảo an toàn, bảo mật khi triển khai các dịch vụ CNTT của ngành Ngân hàng trên nền tảng điện toán đám mây.

Các nội dung nêu trên là những vấn đề quan trọng, nhạy cảm, do đó các quy định liên quan tại Mục 6 Dự thảo Thông tư cần được xem xét thận trọng, cân bằng giữa lợi ích và rủi ro của dịch vụ điện toán đám mây nói riêng và sử dụng dịch vụ của bên thứ ba nói chung.

1. **Trách nhiệm thi hành**

Thông tư 31/2015/TT-NHNN được quy định áp dụng chung cho các đối tượng như tổ chức tín dụng trong nước, chi nhánh ngân hàng nước ngoài và tổ chức trung gian thanh toán. Tuy nhiên với mỗi loại hình đơn vị có những đặc điểm riêng, do vậy để đảm bảo tính khả thi đề nghị các đơn vị rà soát, cho ý kiến góp ý cụ thể về các quy định sẽ gây vướng mắc, khó khăn cho hoạt động của đơn vị./.

**CỤC CÔNG NGHỆ THÔNG TIN**