|  |  |
| --- | --- |
| **NGÂN HÀNG NHÀ NƯỚC****VIỆT NAM**  | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM****Độc lập - Tự do - Hạnh phúc** |

**QUY CHẾ**

**QUẢN LÝ VÀ SỬ DỤNG DỊCH VỤ ĐIỆN TOÁN ĐÁM MâY**

**TRONG NGÀNH NGÂN HÀNG**

1. **I – NHỮNG QUY ĐỊNH CHUNG**
2. **Phạm vi điều chỉnh**

Quy chế này hướng dẫn việc thuê ngoài, quản lý và sử dụng dịch vụ điện toán đám mây trong ngành ngân hàng.

Các hoạt động ứng dụng điện toán đám mây do Tổ chức tự xây dựng để cung cấp dịch vụ điện toán đám mây riêng phục vụ cho Tổ chức thì không phải tuân thủ các quy định tại Quy chế này.

1. **Đối tượng áp dụng**

Quy chế này áp dụng đối với các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài và các tổ chức cung ứng dịch vụ trung gian thanh toán (sau đây gọi chung là Tổ chức) có hoạt động thuê ngoài dịch vụ điện toán đám.

1. **Giải thích từ ngữ**

*Điện toán đám mây (Cloud computing):* là mô hình cung cấp các tài nguyên máy tính (tính toán, xử lý và lưu trữ) dưới dạng dịch vụ (thay vì dưới dạng sản phẩm) qua môi trường mạng.

*Điện toán đám mây công cộng (Public cloud computing)*: là mô hình điện toán đám mây được cung cấp qua một mạng máy tính mở, chia sẻ cho nhiều Tổ chức, người sử dụng.

*Điện toán đám mây riêng (Private cloud computing)*: là mô hình điện toán đám mây do Tổ chức xây dựng để cung cấp dịch vụ điện toán đám mây phục vụ riêng cho Tổ chức đó.

*Điện toán đám mây lai (Hybrid cloud computing):* là mô hình điện toán đám mây kết hợp giữa điện toán đám mây công cộng và điện toán đám mây riêng.

*Dịch vụ điện toán đám mây* (sau đây gọi là Dịch vụ đám mây): là việc cung cấp tài nguyên máy tính, tính toán, xử lý và lưu trữ dưới dạng dịch vụ qua môi trường mạng; cho phép khách hàng có thể điều chỉnh cấu hình theo nhu cầu[[1]](#footnote-1) và thanh toán theo nhu cầu sử dụng.

*Mô hình dịch vụ đám mây* là các sản phẩm dịch vụ điện toán đám mây có thể cung cấp bao gồm: dịch vụ cung cấp cơ sở hạ tầng theo mô hình điện toán đám mây - Infrastructure-as-a-Service (IaaS); dịch vụ cung cấp nền tảng theo mô hình điện toán đám mây- Platform-as-a-Service (PaaS); và dịch vụ cung cấp phần mềm theo mô hình điện toán đám mây - Software-as-a-Service (SaaS).

*Nhà cung cấp dịch vụ điện toán đám mây* (sau đây gọi là Nhà cung cấp dịch vụ)*:* là doanh nghiệp[[2]](#footnote-2) cung cấp dịch vụ đám mây cho các Tổ chức.

1. **Nguyên tắc sử dụng dịch vụ đám mây**

Việc sử dụng dịch vụ đám mây phục vụ các hoạt động ngân hàng phải chịu sự quản lý, giám sát của Ngân hàng Nhà nước.

Việc sử dụng dịch vụ đám mây không làm thay đổi nghĩa vụ của Tổ chức trong việc cung cấp thông tin, báo cáo theo quy định của pháp luật, Ngân hàng Nhà nước.

Việc sử dụng dịch vụ đám mây không làm thay đổi khả năng cung cấp dịch vụ liên tục của Tổ chức cho khách hàng;

Việc sử dụng dịch vụ đám mây không ảnh hưởng đến hình ảnh, tín nhiệm của Tổ chức.

Việc sử dụng dịch vụ đám mây không làm suy giảm việc kiểm soát quy trình nghiệp vụ và không vi phạm Quy chế bảo mật, an toàn hệ thống công nghệ thông tin của Tổ chức;

Việc sử dụng dịch vụ đám mây không làm thay đổi trách nhiệm của các Tổ chức trong việc bảo đảm an toàn, bí mật thông tin. Tổ chức phải chủ động trong việc phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời các tình huống, hành vi đe dọa an toàn hệ thống công nghệ thông tin.

Trong quá trình sử dụng dịch vụ đám mây, các Tổ chức có trách nhiệm phối hợp, hợp tác chặt chẽ với các cơ quan chức năng có thẩm quyền để xử lý các sự cố, hành vi vi phạm an toàn hệ thống công nghệ thông tin (nếu có).

1. **II – PHẠM VI VÀ ĐIỀU KIỆN SỬ DỤNG DỊCH VỤ ĐÁM MÂY**
2. **Phạm vi sử dụng dịch vụ đám mây**

Tổ chức tự quyết định lựa chọn, sử dụng mô hình dịch vụ đám mây. Tổ chức không được sử dụng dịch vụ đám mây để xử lý, lưu trữ các dữ liệu MẬT, TỐI MẬT, TUYỆT MẬT theo quy định bảo vệ bí mật nhà nước trong ngành Ngân hàng.

1. **Điều kiện sử dụng dịch vụ đám mây**

Trước khi quyết định sử dụng dịch vụ đám mây, Tổ chức phải thực hiện các công việc sau:

Phân loại dữ liệu theo thuộc tính bí mật. Lựa chọn hoạt động, chức năng, quy trình, hệ thống, sản phẩm dịch vụ của Tổ chức dự kiến triển khai trên dịch vụ đám mây; lựa chọn mô hình, dữ liệu đưa lên dịch vụ đám mây tuân thủ quy định tại Điều 5 Quy chế này.

Đánh giá rủi ro công nghệ thông tin, rủi ro hoạt động trước khi sử dụng dịch vụ đám mây, chi tiết tại Điều 7 Quy chế này.

Rà soát và hoàn thiện các chính sách quản lý rủi ro của Tổ chức.

Xây dựng tiêu chí lựa chọn Nhà cung cấp dịch vụ đám mây, chi tiết tại Điều 8 Quy chế này.

1. **III – TRƯỚC KHI SỬ DỤNG DỊCH VỤ ĐÁM MÂY**
2. **Đánh giá rủi ro công nghệ thông tin, rủi ro hoạt động**

Tổ chức phải thực hiện đánh giá rủi ro công nghệ thông tin, rủi ro hoạt động trước khi sử dụng dịch vụ đám mây bao gồm các nội dung tối thiểu sau:

Nhận diện rủi ro, phân tích, ước lượng mức độ tổn hại, mối đe dọa đến an toàn, bảo mật hệ thống công nghệ thông tin; khả năng cung cấp dịch vụ liên tục cho khách hàng; khả năng thực hiện nghĩa vụ báo cáo, cung cấp thông tin theo quy định của Ngân hàng Nhà nước;

Xác định rõ vai trò, trách nhiệm của các bên liên quan khi sử dụng dịch vụ;

Xây dựng các biện pháp nhằm giảm thiểu rủi ro, biện pháp ứng cứu, khắc phục sự cố.

1. **Tiêu chí lựa chọn Nhà cung cấp**

Tổ chức phải xây dựng tiêu chí lựa chọn Nhà cung cấp. Tiêu chí lựa chọn Nhà cung cấp bao gồm các nội dung tối thiểu sau:

Đáp ứng yêu cầu về an toàn công nghệ thông tin: đạt chứng nhận ISO/IEC 27001 hoặc tương đương hoặc đáp ứng các các quy định hiện hành về đảm bảo an toàn thông tin của Pháp luật và của Ngân hàng Nhà nước. Tham khảo Mục A – Các quy định hiện hành của NHNN nhằm đảm bảo an toàn công nghệ thông tin trong hoạt động ngân hàng *(Phụ lục 01 đính kèm Quy chế này)*.

Đáp ứng yêu cầu về an toàn công nghệ thông tin khi cung cấp dịch vụ đám mây: Đảm bảo Đạt chứng nhận ISO/IEC 27017 hoặc tương đương. Tổ chức sử dụng mô hình điện toán đám mây nào thì hạ tầng công nghệ thông tin cung cấp dịch vụ đám mây đó phải đảm bảo tuân thủ các quy định hiện hành của Nhà nước và của Ngân hàng Nhà nước. Tham khảo Mục B – Mô hình dịch vụ đám mây và các quy định hiện hành tương ứng cần tuân thủ *(Phụ lục 01 đính kèm Quy chế này)*.

Năng lực, danh tiếng và kinh nghiệm của Nhà cung cấp dịch vụ đối với sản phẩm dịch vụ mà Tổ chức dự kiến sử dụng;

Nhà cung cấp dịch vụ là doanh nghiệp được thành lập và hoạt động theo pháp luật Việt Nam. Trường hợp Nhà cung cấp bên ngoài lãnh thổ Việt Nam, Tổ chức phải:

Bổ sung các tiêu chí về chính sách, điều kiện kinh tế và pháp lý của quốc gia/vùng lãnh thổ nơi Nhà cung cấp đăng ký kinh doanh.

Cung cấp ý kiến đánh giá về khả năng tuân thủ các điều kiện tại Hợp đồng của Nhà cung cấp của ít nhất 01 tổ chức cố vấn pháp lý có kinh nghiệm cố vấn các hợp đồng quốc tế.

Gửi hồ sơ đánh giá, lựa chọn Nhà cung cấp dịch vụ xin ý kiến Ngân hàng Nhà nước trước khi ký hợp đồng sử dụng dịch vụ. Việc ký hợp đồng sử dụng dịch vụ phải được sự đồng ý của Ngân hàng Nhà nước.

Trường hợp Trung tâm dữ liệu của Nhà cung cấp dịch vụ nằm ngoài lãnh thổ Việt Nam, Tổ chức cân nhắc việc xây dựng các tiêu chí quy định cụ thể các vị trí lưu trữ dữ liệu triển khai trên dịch vụ đám mây. Vị trí lưu trữ dữ liệu phải đáp ứng các yêu cầu về việc thực hiện nghĩa vụ cung cấp thông tin, báo cáo theo quy định của Ngân hàng Nhà nước.

1. **Hợp đồng sử dụng dịch vụ đám mây**

Hợp đồng ký kết với Nhà cung cấp dịch vụ đám mây cần có những điều khoản quy định những nội dung tối thiểu sau đây:

Cam kết của Nhà cung cấp dịch vụ về bảo đảm an toàn công nghệ thông tin:

Đáp ứng yêu cầu quy định tại Khoản 1, Khoản 2 Điều 8 Quy chế này.

KHÔNG sao chép, thay đổi, sử dụng hay cung cấp dữ liệu triển khai trên dịch vụ đám mây cho Bên thứ ba ngoài mục đích cung cấp dịch vụ đám mây cho Tổ chức.

Quyền kiểm tra sự tuân thủ quy định bảo đảm an toàn công nghệ thông tin: Nhà cung cấp dịch vụ phải cho phép Tổ chức, Ngân hàng Nhà nước hoặc Tổ chức kiểm toán độc lập thực hiện việc kiểm tra tuân thủ an toàn công nghệ thông tin. Nhà cung cấp phải chia sẻ, cung cấp kết quả kiểm tra an toàn công nghệ thông tin của các Tổ chức kiểm toán độc lập.

Hỗ trợ điều tra: Nhà cung cấp dịch vụ phải hỗ trợ, hợp tác điều tra trong trường hợp có yêu cầu từ các cơ quan chức năng có thẩm quyền thực hiện xử lý các sự cố vi phạm an toàn thông tin mạng theo quy định của pháp luật.

Sở hữu dữ liệu: Dữ liệu triển khai trên dịch đám mây, phát sinh thêm trong quá trình triển khai, sử dụng dịch vụ đám mây là tài sản của Tổ chức.

Phân tách dữ liệu: Dữ liệu của Tổ chức triển khai trên dịch vụ đám mây phải được tách biệt với dữ liệu của cá nhân, tổ chức khác sử dụng cùng nền tảng kỹ thuật của Nhà cung cấp dịch vụ.

Vị trí đặt dữ liệu: Nhà cung cấp dịch vụ phải minh bạch các vị trí đặt dữ liệu triển khai trên dịch vụ đám mây cho Tổ chức.

Giám sát và kiểm soát chất lượng dịch vụ đám mây: Tổ chức phải yêu cầu Nhà cung cấp dịch vụ cung cấp: (i) Công cụ kiểm soát chất lượng dịch vụ đám mây; (ii) Quy trình giám sát, kiểm soát chất lượng dịch vụ đám mây; (iii) Các đại lượng đo và giá trị để đánh giá chất lượng dịch vụ.

Chất lượng dịch vụ: Quy định cụ thể về thời gian gián đoạn dịch vụ, thời gian khắc phục sự cố, các yêu cầu liên quan đến đảm bảo 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.

Kênh phân phối dịch vụ từ Nhà cung cấp dịch vụ đến Tổ chức: Kênh phân phối dịch vụ phải có biện pháp kỹ thuật để bảo vệ thông tin, xác thực người sử dụng.

Nhà thầu phụ: Trong trường hợp Nhà cung cấp dịch vụ sử dụng Nhà thầu phụ thực hiện bất kỳ nội dung công việc nào thuộc phạm vi dịch vụ đám mây đều phải được thể hiện trong hợp đồng. Việc sử dụng Nhà thầu phụ không làm thay đổi trách nhiệm của Nhà cung cấp dịch vụ đối với sản phẩm dịch vụ đám mây mà Tổ chức sử dụng.

Chấm dứt sử dụng dịch vụ: Tổ chức phải yêu cầu Nhà cung cấp dịch vụ có trách nhiệm:

Trả lại toàn bộ dữ liệu triển khai trên dịch vụ đám mây;

Thực hiện xoá vĩnh viễn dữ liệu trên dịch vụ đám mây;

Trước khi Nhà cung cấp thực hiện xoá vĩnh viễn dữ liệu phải có xác nhận của Tổ chức.

**CHƯƠNG IV – QUẢN LÝ VÀ SỬ DỤNG DỊCH VỤ ĐÁM MÂY**

1. **Quản lý tài sản công nghệ thông tin**

Thông tin, dữ liệu được chứa đựng trong quá trình triển khai, sử dụng dịch vụ đám mây là tài sản thông tin của Tổ chức. Tổ chức phải áp dụng các quy định hiện hành về quản lý tài sản công nghệ thông tin đối với các tài sản triển khai trên dịch vụ đám mây.

1. **Kiểm soát thiết bị truy cập sử dụng dịch vụ đám mây**

Tổ chức phải có biện pháp kỹ thuật để giám sát và kiểm soát các thiết bị của người dùng của Tổ chức sử dụng đồng thời dịch vụ đám mây và xử lý các nghiệp vụ ngân hàng có dữ liệu MẬT, TỐI MẬT, TUYỆT MẬT nhằm giảm thiểu nguy cơ tấn công mạng.

1. **Giám sát hoạt động dịch vụ đám mây**

Tổ chức phải có quy trình, công cụ và tổ chức nguồn lực để giám sát, kiểm soát chất lượng dịch vụ đám mây.

1. **Kiểm tra tuân thủ với Nhà cung cấp dịch vụ**

Tổ chức phải thực hiện đánh giá sự tuân thủ các quy định hiện hành về bảo đảm an toàn công nghệ thông tin của Nhà cung cấp dịch vụ định kỳ 12 tháng / 1 lần. Việc đánh giá sự tuân thủ được thực hiện bằng cách sử dụng kết quả kiểm toán của Tổ chức kiểm toán độc lập.

 Phạm vi kiểm tra tuân thủ tối thiểu bao gồm: tất cả các cơ sở, hệ thống, quy trình của Nhà cung cấp dịch vụ liên quan đến dịch vụ đám mây mà Tổ chức sử dụng.

1. **Chế độ báo cáo**

Trước khi sử dụng dịch vụ đám mây: Tổ chức có trách nhiệm cung cấp thông tin về sử dụng dịch vụ đám mây cho Ngân hàng Nhà nước (thông qua Cục Công nghệ thông tin) tối thiểu 02 tuần trước khi ký hợp đồng sử dụng dịch vụ đám mây. Nội dung thông báo thực hiện theo Mẫu số 01 tại Phụ lục 02 đính kèm Quy chế này.

Báo cáo đột xuất:

Tổ chức có trách nhiệm cung cấp thông tin, báo cáo Ngân hàng Nhà nước (thông qua Cục Công nghệ thông tin) các sự cố, rủi ro trong quá trình sử dụng dịch vụ đám mây làm gián đoạn hoạt động nghiệp vụ; các sự cố liên quan đến mất an toàn công nghệ thông tin của Tổ chức; các sự cố liên quan đến thất thoát, thay đổi thông tin, tài sản công nghệ thông tin của Tổ chức. Thời gian cung cấp thông tin chậm nhất sau 05 ngày làm việc kể từ khi phát sinh sự cố. Nội dung báo cáo thực hiện theo Mẫu số 02 tại Phụ lục 02 đính kèm Quy chế này.

Khi sử dụng dịch vụ đám mấy, nếu có bất kỳ thay đổi nào về Nhà cung cấp dịch vụ, Tổ chức có trách nhiệm gửi thông báo cho Ngân hàng Nhà nước (Cục Công nghệ thông tin) tối thiểu hai (02) tuần trước khi ký hợp đồng sử dụng dịch vụ đám mây với Nhà cung cấp dịch vụ. Nội dung báo cáo thực hiện theo Mẫu số 03 tại Phụ lục 02 đính kèm Quy chế này.

1. **V – TỔ CHỨC THỰC HIỆN**
2. **Hiệu lực thi hành**

Quy chế này có hiệu lực thi hành kể từ ngày …/…/2017, Trong quá trình thực hiện nếu có phát sinh, vướng mắc Tổ chức gửi thông tin về Ngân hàng Nhà nước (Cục Công nghệ thông tin) để xem xét, bổ sung, sửa đổi.

1. **Trách nhiệm thi hành**

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 Quy chế này.

 **THỐNG ĐỐC**

1. Tham khảo dự thảo Nghị đinh về dịch vụ CNTT năm 2012. [↑](#footnote-ref-1)
2. Luật Doanh nghiệp số 68/2014/QH13 quy định Doanh nghiệp là tổ chức có tên riêng, có trụ sở giao dịch được đăng ký thành lập theo quy định của pháp luật nhằm mục đích kinh doanh. [↑](#footnote-ref-2)