| BỘ THÔNG TIN VÀ TRUYỀN THÔNG | CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|
| Số: 2612/BTTTT-CATTT<br>V/v bổ sung bộ tiêu chí, chỉ tiêu để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử | *Hà Nội, ngày 17 tháng 7 năm 2021* |

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước;
- Các Ngân hàng TMCP; Các tổ chức tài chính.

Thực hiện chức năng quản lý nhà nước về an toàn thông tin của Bộ Thông tin và Truyền thông tại Nghị định số 17/2017/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 Bộ Thông tin và Truyền thông;

Thực hiện Nghị quyết số 17/NQ-CP ngày 07 tháng 3 năm 2019 của Chính phủ về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử giai đoạn 2019- 2020, định hướng đến 2025;

Thực hiện Quyết định số 942/QĐ-TTg ngày 15 tháng 6 năm 2021 của Chính phủ về phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030;

Ngày 03/4/2020, Bộ Thông tin và Truyền thông ban hành văn bản số 1145/BTTTT-CATTT về việc "Hướng dẫn bộ tiêu chí, chỉ tiêu kỹ thuật để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử";

Bộ Thông tin và Truyền thông ban hành văn bản "Bổ sung bộ tiêu chí, chỉ tiêu để đánh giá và lựa chọn giải pháp nền tảng điện toán đám mây phục vụ Chính phủ điện tử/Chính quyền điện tử". Cơ quan, tổ chức căn cứ vào hướng dẫn trong tài liệu này và văn bản số 1145/BTTTT-CATTT ban hành ngày 03/4/2020 làm cơ sở để đánh giá, lựa chọn giải pháp hoặc thuê dịch vụ nền tảng điện toán đám mây phục vụ phát triển Chính phủ điện tử/Chính quyền điện tử.

Bản mềm tài liệu hướng dẫn có thể được tải về từ cổng thông tin điện tử của Bộ Thông tin và Truyền thông tại địa chỉ: http://www.mic.gov.vn.

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc đề nghị các cơ quan, tổ chức gửi ý kiến về Bộ Thông tin và Truyền thông qua (Cục An toàn thông tin) để được hướng dẫn, phối hợp và hỗ trợ.

Chi tiết xin liên hệ: Cục An toàn thông tin, Điện thoại: 02432096789; Thư điện tử: GV_cloud@mic.gov.vn;

Trân trọng cảm ơn./.

***Nơi nhận:***
- Như trên;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng Thông tin điện tử Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện kiểm sát nhân dân tối cao, Kiểm toán nhà nước;
- Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương;
- Cổng thông tin điện tử Bộ TT&TT;
- Lưu: VT, CATTT.

**KT. BỘ TRƯỞNG**
**THỨ TRƯỞNG**

**Nguyễn Huy Dũng**

# BỔ SUNG BỘ TIÊU CHÍ, CHỈ TIÊU ĐỂ ĐÁNH GIÁ VÀ LỰA CHỌN GIẢI PHÁP NỀN TẢNG ĐIỆN TOÁN ĐÁM MÂY PHỤC VỤ CHÍNH PHỦ ĐIỆN TỬ/CHÍNH QUYỀN ĐIỆN TỬ

*(Kèm theo Công văn số 2612/BTTTT-CATTT ngày 17 tháng 7 năm 2021 của Bộ Thông tin và Truyền thông)*

## I. Quyền truy cập vào dữ liệu của khách hàng sử dụng dịch vụ điện toán đám mây bởi nhân viên của nhà cung cấp dịch vụ

### 1. Thiết lập chính sách an toàn thông tin

a) Xây dựng chính sách bảo mật thông tin cơ bản áp dụng cho việc thiết kế và triển khai dịch vụ đám mây;

b) Xây dựng chính sách Quyền truy cập vào tài sản của khách hàng dịch vụ đám mây bởi nhân viên của nhà cung cấp dịch vụ đám mây;

c) Xây dựng chính sách Truy cập và bảo vệ dữ liệu khách hàng dịch vụ đám mây.

### 2. Tổ chức bảo mật thông tin

a) Chỉ định bộ phận chuyên trách theo dõi chặt chẽ và có phương án kiểm soát độc lập nhằm đảm bảo phát hiện, không một cá nhân nào có thể truy cập trái phép vào vùng vật lý, địa lý nơi có dữ liệu tài sản của khách hàng, chỉnh sửa hoặc sử dụng tài sản khi chưa được phép hoặc không bị phát hiện.

b) Áp dụng nguyên tắc này đến mức có thể và khả thi.

### 3. Sự tuân thủ

#### 3.1. Sự tuân thủ các yêu cầu pháp lý và hợp đồng

a) Yêu cầu về pháp lý, quy định, nghĩa vụ trong hợp đồng đã ký và cách tiếp cận của tổ chức để đáp ứng với những yêu cầu này phải được xác định rõ ràng, lập thành tài liệu và được cập nhật thường xuyên đối với mỗi hệ thống thông tin và tổ chức;

b) Triển khai các thủ tục phù hợp nhằm đảm bảo sự phù hợp với các yêu cầu pháp lý, các quy định và cam kết theo hợp đồng trong việc sử dụng các tài liệu có quyền sở hữu trí tuệ và các sản phẩm phần mềm độc quyền; thiết lập một quy trình để đáp ứng các khiếu nại các quyền sở hữu trí tuệ.

c) Các hồ sơ quan trọng cần được bảo vệ khỏi sự mất mát, phá hủy, làm sai lệch, truy cập và tiết lộ trái phép, phù hợp với pháp luật, quy định, các nghĩa vụ trong hợp đồng đã ký; cung cấp thông tin cho khách hàng dịch vụ đám mây về

việc bảo vệ hồ sơ được thu thập và lưu trữ bởi nhà cung cấp dịch vụ đám mây liên quan đến việc sử dụng dịch vụ đám mây của khách hàng dịch vụ đám mây.

d) Đảm bảo việc bảo vệ dữ liệu và tính riêng tư theo yêu cầu pháp lý, quy định khi áp dụng;

đ) Quản lý mật mã cần được áp dụng phù hợp với các thỏa thuận, luật pháp và các quy định liên quan; cung cấp các mô tả về biện pháp kiểm soát mật mã đã triển khai bởi nhà cung cấp dịch vụ đám mây với khách hàng để xem xét việc tuân thủ các thỏa thuận, pháp luật và quy định hiện hành.

**3.2. Soát xét về an toàn thông tin**

a) Soát xét các mục tiêu, biện pháp, chính sách và quy trình an toàn thông tin một cách độc lập tại các khoảng thời gian được lên kế hoạch hoặc khi có thay đổi;

b) Soát xét sự tuân thủ của việc xử lý thông tin và thủ tục trong khu vực trách nhiệm của mình với các chính sách an toàn thích hợp, các tiêu chuẩn và yêu cầu an toàn khác;

c) Soát xét thường xuyên các hệ thống thông tin về sự tuân của các chính sách và tiêu chuẩn an toàn thông tin của tổ chức.

**II. Truy cập và bảo vệ dữ liệu khách hàng dịch vụ đám mây**

**4. Kiểm soát truy cập**

**4.1. Yêu cầu nghiệp vụ đối với kiểm soát truy cập**

a) Xây dựng chính sách kiểm soát truy cập cần được thiết lập, lập tài liệu và soát xét dựa trên các yêu cầu nghiệp vụ và an toàn đối với các truy cập;

b) Quy định người dùng chỉ được truy cập vào mạng và sử dụng các dịch vụ mạng mà họ đã được cấp phép.

**4.2. Kiểm soát truy cập người dùng**

a) Cung cấp các chức năng đăng ký và xóa đăng ký người sử dụng và các đặc tả kỹ thuật của việc sử dụng các chức năng này cho khách hàng dịch vụ đám mây;

b) Cung cấp các chức năng để quản lý các quyền truy cập của người sử dụng dịch vụ đám mây của khách hàng dịch vụ đám mây và các đặc tả kỹ thuật cho việc sử dụng các chức năng này;

c) Cung cấp đầy đủ các kỹ thuật xác thực để đảm bảo chính xác một quản trị viên có quyền quản trị một dịch vụ đám mây hay không;

d) Cung cấp thông tin về quy trình quản lý xác thực thông tin bí mật của khách hàng dịch vụ đám mây, bao gồm các thủ tục để phân bổ thông tin đó và để xác thực người dùng;

đ) Định kỳ soát xét các quyền truy cập của người dùng;

e) Khi chấm dứt hợp đồng, các quyền truy cập thông tin của các cá nhân đối với thông tin và các tài sản đi kèm với các phương tiện xử lý thông tin và dịch vụ phải được huỷ bỏ hoặc đình chỉ.

**4.3. Các trách nhiệm của người dùng**

Yêu cầu người dùng phải tuân thủ quy tắc thực hành an toàn của tổ chức trong việc sử dụng các thông tin xác thực bí mật.

**4.4. Kiểm soát truy cập vào hệ thống và ứng dụng**

a) Cung cấp các biện pháp kiểm soát truy cập cho phép khách hàng sử dụng dịch vụ đám mây hạn chế quyền truy cập vào các dịch vụ đám mây, các chức năng dịch vụ đám mây và dữ liệu khách hàng dịch vụ đám mây được duy trì trong dịch vụ;

b) Truy cập vào hệ thống và ứng dụng cần được kiểm soát bởi thủ tục đăng nhập an toàn;

c) Các hệ thống quản lý mật khẩu phải có khả năng tương tác và đảm bảo độ khó của mật khẩu;

d) Việc sử dụng các chương trình tiện ích có khả năng ảnh hưởng đến việc quản lý hệ thống và các chương trình ứng dụng khác phải được giới hạn và kiểm soát chặt chẽ; xác định các yêu cầu đối với bất kỳ chương trình tiện ích nào được sử dụng trong dịch vụ đám mây;

đ) Giới hạn chặt chẽ việc truy cập đến mã nguồn của chương trình.

**5. An toàn vận hành**

**5.1. Các quy trình và trách nhiệm vận hành**

a) Lập tài liệu, duy trì các thủ tục vận hành và luôn sẵn sàng đối với mọi người cần dùng đến;

b) Kiểm soát các thay đổi đối với tổ chức, quy trình nghiệp vụ, các phương tiện và hệ thống xử lý thông tin có ảnh hưởng đến an toàn thông tin; cung cấp cho khách hàng dịch vụ đám mây thông tin liên quan đến thay đổi với dịch vụ đám mây mà có thể ảnh hưởng xấu đến dịch vụ đám mây;

c) Theo dõi, điều chỉnh và thực hiện dự báo các yêu cầu năng lực trong tương lai về việc sử dụng các nguồn tài nguyên để đảm bảo hiệu quả vận hành hệ thống; giám sát tổng công suất của nguồn lực để ngăn ngừa các sự cố an toàn thông tin gây ra bởi sự thiếu hụt nguồn lực;

d) Phân tách các chức năng phát triển, kiểm thử và môi trường vận hành nhằm giảm thiểu các rủi ro do truy cập hoặc thay đổi môi trường vận hành trái phép.

**5.2. Bảo vệ khỏi phần mềm độc hại**

Thực hiện, kết hợp với nhận thức về việc phát hiện, phòng ngừa và phục hồi quyền điều khiển.

**5.3. Sao lưu**

Thực hiện và kiểm tra thường xuyên bản sao lưu các thông tin, phần mềm và image/bản chụp snapshot của hệ thống.

**5.4. Ghi nhật ký và giám sát**

a) Lưu giữ và thường xuyên soát xét nhật ký các sự kiện ghi lại các thao tác người sử dụng, các trường hợp ngoại lệ, lỗi và sự cố an toàn thông tin cần được tạo ra;

b) Bảo vệ chống sửa đổi và truy cập trái phép các thiết bị lưu vết và thông tin nhật ký;

c) Bảo vệ an toàn và thường xuyên rà soát các hoạt động của người quản trị và người điều hành hệ thống;

d) Đồng bộ hóa các đồng hồ của tất cả hệ thống xử lý thông tin liên quan đến tổ chức bởi một nguồn tham chiếu duy nhất.

**5.5. Kiểm soát phần mềm điều hành**

Kiểm soát việc cài đặt phần mềm trên các hệ thống hoạt động.

**5.6. Quản lý lỗ hổng kỹ thuật**

a) Thu thập, đánh giá và đưa ra các biện pháp thích hợp về các lỗ hổng kỹ thuật của hệ thống;

b) Thiết lập và thực hiện quy định điều chỉnh cài đặt phần mềm bởi những người sử dụng.

**5.7. Soát xét việc đánh giá các hệ thống thông tin**

Đánh giá và các hành động liên quan đến việc xác thực hệ thống hoạt động cần được lên kế hoạch cẩn thận và thống nhất.

**6. Quản lý vận hành hệ thống**

a) Thiết lập các thủ tục và trách nhiệm quản lý đảm bảo sự phản ứng nhanh chóng, hiệu quả, đúng trình tự khi xảy ra các sự cố an toàn thông tin;

b) Báo cáo các sự kiện an toàn thông tin thông qua các kênh quản lý thích hợp;

c) Yêu cầu đối với mọi nhân viên và người sử dụng dịch vụ điện toán đám mây ghi lại các báo cáo lỗ hổng về an toàn quan sát;

d) Đánh giá, phân loại các sự kiện an toàn thông tin;

đ) Ứng phó phù hợp với các thủ tục đã được lập tài liệu các sự cố an toàn thông tin;

e) Phân tích và giải quyết các sự cố an toàn thông tin cần được sử dụng;

g) Xác định và áp dụng các thủ tục cho việc xác định, tập hợp, thu nhận, bảo quản thông tin có thể phục vụ làm bằng chứng./.