

BỘ CÔNG AN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: **8297** /QĐ-BCA-A05

Hà Nội, ngày **09** tháng **10** năm 2025

QUYẾT ĐỊNH

Ban hành Bộ tiêu chí đảm bảo an ninh mạng đối với nền tảng điện toán đám mây phục vụ Chính phủ điện tử/ Chính quyền điện tử

BỘ TRƯỞNG BỘ CÔNG AN

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 02/2025/NĐ-CP ngày 18 tháng 2 năm 2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an;

Căn cứ Quyết định số 749/QĐ-TTg ngày 3 tháng 6 năm 2020 của Thủ tướng Chính phủ về việc phê duyệt “Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”;

Căn cứ Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng Chính phủ về việc phê duyệt chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030;

Căn cứ Quyết định số 1035/QĐ-BCA ngày 26 tháng 2 năm 2025 của Bộ trưởng Bộ công an về việc giao nhiệm vụ quản lý nhà nước về an toàn thông tin mạng;

Căn cứ Quyết định số 1121/QĐ-TTg phê duyệt ngày 11 tháng 6 năm 2025 của Thủ tướng Chính phủ về việc phê duyệt “Chương trình hành động quốc gia về phát triển và chuyển đổi sang sử dụng nền tảng điện toán đám mây giai đoạn 2025-2030”;

*Theo đề nghị của Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao tại Tờ trình số **8063** /TTr-A05-TT4 ngày **01** tháng 10 năm 2025.*

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Bộ tiêu chí đảm bảo an ninh mạng đối với nền tảng điện toán đám mây phục vụ Chính phủ điện tử/ Chính quyền điện tử.

Điều 2. Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao chủ trì, phối hợp các đơn vị liên quan hướng dẫn, kiểm tra, đánh giá việc áp dụng các yêu cầu theo Bộ tiêu chí tại Điều 1 Quyết định này.

Điều 3. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 4. Chánh Văn phòng, Cục trưởng Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Thủ trưởng các đơn vị trực thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này. *lưu*

Nơi nhận:

- Như Điều 4 (để thực hiện);
- Các đồng chí Thứ trưởng (để chỉ đạo);
- Cổng Thông tin điện tử Bộ Công an (để đăng tải);
- Lưu: VT, A05(TT4).25b



Đại tướng Lương Tam Quang

BỘ TIÊU CHÍ
ĐẢM BẢO AN NINH MẠNG ĐỐI VỚI NỀN TẢNG ĐIỆN TOÁN Đám Mây
PHỤC VỤ CHÍNH PHỦ ĐIỆN TỬ/ CHÍNH QUYỀN ĐIỆN TỬ

(Kèm theo Quyết định số **8297/QĐ-BCA-A05** ngày **09 / 10 /2025** của
Bộ trưởng Bộ Công an)

I. QUY ĐỊNH CHUNG

1.1. Phạm vi áp dụng

Tài liệu này đưa ra các tiêu chí cơ bản nhằm đảm bảo an ninh mạng đối với nền tảng điện toán đám mây. Căn cứ vào các tiêu chí này, cơ quan, tổ chức có cơ sở để đánh giá, lựa chọn giải pháp dịch vụ điện toán đám mây (sau đây viết tắt là ĐTĐM) phục vụ phát triển Chính phủ điện tử/ Chính quyền điện tử (CPĐT/CQĐT).

1.2. Đối tượng áp dụng

- a) Các cơ quan, tổ chức nhà nước xây dựng, triển khai giải pháp nền tảng điện toán đám mây phục vụ CPĐT/CQĐT.
- b) Doanh nghiệp cung cấp giải pháp, dịch vụ nền tảng điện toán đám mây phục vụ CPĐT/CQĐT.
- c) Khuyến khích cơ quan, tổ chức khác tham khảo để xây dựng, triển khai giải pháp nền tảng điện toán đám mây.

1.3. Thuật ngữ và định nghĩa

1.3.1. Khách hàng dịch vụ điện toán đám mây

Cơ quan, tổ chức nhà nước có hợp đồng thuê/ sử dụng các dịch vụ từ nhà cung cấp dịch vụ điện toán đám mây.

1.3.2. Nhà cung cấp dịch vụ điện toán đám mây

Tổ chức chịu trách nhiệm cung cấp dịch vụ điện toán đám mây cho khách hàng dịch vụ ĐTĐM.

1.3.3. Khách tham quan

Cơ quan, tổ chức, cá nhân không thuộc nhà cung cấp dịch vụ hoặc bộ phận vận hành hệ thống được phép tiếp cận tạm thời khu vực hạ tầng vật lý với mục đích khảo sát, tham quan, đánh giá hoặc công tác; phải tuân thủ các quy định kiểm soát truy cập, an toàn và bảo mật của nhà cung cấp dịch vụ.

1.3.4. Nhật ký khách tham quan

Tài liệu hoặc hệ thống ghi nhận thông tin về các khách tham quan đã được phép vào khu vực hạ tầng vật lý, bao gồm: thời gian vào/ra, danh tính, mục đích, khu vực truy cập, người giám sát, ghi chú liên quan đến an ninh, bảo mật...

1.3.5. Phần mềm trái phép

Những phần mềm không nằm trong danh sách phần mềm được phép sử dụng hoặc đã hết thời gian hỗ trợ của nhà cung cấp, nhà phát triển phần mềm.

1.3.6. Infrastructure as Code (IaC)

Phương pháp quản lý và cung cấp hạ tầng công nghệ thông tin thông qua mã nguồn thay vì các quy trình thủ công.

1.3.7. Vendor lock-in

Tình trạng phụ thuộc vào một nhà cung cấp (dịch vụ, sản phẩm hay nền tảng công nghệ), khiến việc chuyển sang nhà cung cấp khác trở nên khó khăn, do các rào cản như chi phí chuyển đổi cao, kỹ thuật phức tạp hoặc ảnh hưởng nghiêm trọng tới hoạt động.

1.4. Từ viết tắt

STT	Từ viết tắt	Thuật ngữ tiếng Anh	Thuật ngữ tiếng Việt
1	CPĐT/ CQĐT		Chính phủ điện tử/ Chính quyền điện tử
2	ĐTĐM		Điện toán đám mây
3	IaC	Infrastructure as Code	Hạ tầng dưới dạng mã
4	TTDL		Trung tâm dữ liệu
5	IaaS	Infrastructure as a Service	Hạ tầng dưới dạng dịch vụ
6	PaaS	Platform as a Service	Nền tảng dưới dạng dịch vụ
7	SaaS	Software as a Service	Phần mềm dưới dạng dịch vụ
8	FaaS	Function as a Service	Chức năng dưới dạng dịch vụ

II. TỔNG QUAN VỀ NỀN TẢNG ĐIỆN TOÁN ĐÁM MÂY

2.1. Khái niệm điện toán đám mây

a) Điện toán đám mây là mô hình dịch vụ cho phép sử dụng tài nguyên điện toán dùng chung (mạng, máy chủ, lưu trữ, ứng dụng, dịch vụ...) thông qua kết nối mạng. Tài nguyên điện toán đám mây có thể được thiết lập hoặc hủy bỏ bởi người dùng mà không cần sự can thiệp của Nhà cung cấp dịch vụ.

b) Đặc điểm cơ bản của ĐTĐM:

- Tự phục vụ theo yêu cầu (On-demand self-service): Người dùng có thể tự lựa chọn, cung cấp các năng lực tính toán (chẳng hạn như thời gian máy chủ hoặc dung lượng lưu trữ mạng) theo nhu cầu mà không cần sự tương tác trực tiếp với nhà cung cấp dịch vụ.

- Truy cập mạng diện rộng (Broad network access): Các năng lực tính toán được cung cấp qua mạng và truy cập thông qua các giao thức chuẩn, hỗ trợ truy cập cho nhiều loại thiết bị khác nhau (ví dụ: điện thoại di động, máy tính bảng, máy tính xách tay, máy trạm).

- Tài nguyên dùng chung (Resource pooling): Tài nguyên tính toán của nhà cung cấp dịch vụ được gom lại để phục vụ nhiều người dùng theo mô hình đa thuê (multi-tenant). Các tài nguyên vật lý và ảo khác nhau được phân bổ và tái phân bổ tùy theo nhu cầu của người dùng. Đặc tính này thể hiện sự độc lập về vị trí, nghĩa là khách hàng không kiểm soát hoặc không biết chính xác vị trí tài nguyên được cung cấp nhưng có thể chỉ định vị trí ở mức trừu tượng cao hơn (ví dụ: quốc gia hoặc trung tâm dữ liệu). Các loại tài nguyên bao gồm: lưu trữ, xử lý, bộ nhớ và băng thông mạng.

- Khả năng đáp ứng yêu cầu thay đổi nhanh chóng (Rapid elasticity): Các năng lực tính toán có thể được mở rộng hoặc thu hẹp linh hoạt, trong một số trường hợp có thể tự động điều chỉnh để đáp ứng nhanh chóng theo nhu cầu. Với người dùng, các tài nguyên này thường có vẻ như là vô hạn và có thể được khai thác với bất kỳ số lượng nào, vào bất kỳ thời điểm nào.

- Kiểm soát dịch vụ (Measured service): Hệ thống đám mây tự động kiểm soát và tối ưu hóa việc sử dụng tài nguyên bằng cách áp dụng cơ chế đo lường ở các mức trừu tượng phù hợp với từng loại dịch vụ (ví dụ: lưu trữ, xử lý, băng thông, số lượng tài khoản người dùng hoạt động). Việc sử dụng tài nguyên có thể được giám sát, kiểm soát và báo cáo, bảo đảm tính minh bạch cho cả nhà cung cấp và người sử dụng dịch vụ.

2.2. Phân loại một số phương pháp triển khai ĐTĐM

a) Đám mây công cộng (Public Cloud): Hạ tầng đám mây được cung cấp cho mọi đối tượng người dùng, không hạn chế. Đám mây công cộng có thể thuộc sở hữu, quản lý và vận hành bởi tổ chức doanh nghiệp, cơ quan chính phủ hoặc kết hợp giữa các tổ chức này. Hạ tầng này được triển khai trên cơ sở hạ tầng của nhà cung cấp dịch vụ ĐTĐM.

b) Đám mây riêng (Private Cloud): Hạ tầng đám mây được cung cấp dành riêng cho một tổ chức, có thể phục vụ nhiều người dùng trong tổ chức đó (ví dụ: các phòng/ban nghiệp vụ). Đám mây riêng có thể thuộc sở hữu, quản lý và vận hành bởi chính tổ chức đó, bởi bên thứ ba, hoặc kết hợp giữa các bên; đồng thời có thể được triển khai tại chỗ (on-premises) hoặc bên ngoài (off-premises).

c) Đám mây lai (Hybrid Cloud): Hạ tầng đám mây được tạo thành từ hai hoặc nhiều hạ tầng đám mây riêng biệt (riêng, cộng đồng, hoặc công cộng), duy trì tính độc lập nhưng được kết nối với nhau thông qua công nghệ tiêu chuẩn hóa hoặc công nghệ độc quyền, cho phép di chuyển dữ liệu và ứng dụng (ví dụ: cloud bursting để cân bằng tải giữa các đám mây).

d) Đám mây cộng đồng (Community Cloud): Hạ tầng đám mây được cung cấp dành riêng cho một cộng đồng người dùng từ nhiều tổ chức khác nhau có cùng mối quan tâm chung (ví dụ: nhiệm vụ, yêu cầu an toàn thông tin, chính sách quản lý, hoặc tuân thủ quy định pháp luật). Đám mây cộng đồng có thể thuộc sở hữu, được quản lý và vận hành bởi một hoặc nhiều tổ chức trong cộng đồng, bởi bên thứ ba, hoặc kết hợp giữa các bên; đồng thời có thể được triển khai tại chỗ hoặc bên ngoài.

2.3. Phân loại các mô hình cung cấp dịch vụ ĐTĐM

a) Hạ tầng dưới dạng dịch vụ (**IaaS** – Infrastructure as a Service): Cấp phát các tài nguyên tính toán cơ bản như xử lý, lưu trữ, mạng và các tài nguyên hạ tầng khác, cho phép người dùng triển khai và vận hành phần mềm tùy ý, bao gồm hệ điều hành và ứng dụng. Người dùng không quản lý hay kiểm soát hạ tầng đám mây bên dưới, nhưng có toàn quyền kiểm soát đối với hệ điều hành, lưu trữ, các ứng dụng đã triển khai và có thể có quyền hạn giới hạn đối với một số thành phần mạng (ví dụ: tường lửa máy chủ).

b) Nền tảng dưới dạng dịch vụ (**PaaS** - Platform as a Service): Triển khai các ứng dụng do chính người dùng phát triển hoặc mua ngoài lên hạ tầng đám mây bằng cách sử dụng các ngôn ngữ lập trình, thư viện, dịch vụ và công cụ được nhà cung cấp dịch vụ hỗ trợ. Người dùng không quản lý hay kiểm soát hạ tầng đám mây bên dưới, bao gồm mạng, máy chủ, hệ điều hành hoặc lưu trữ, nhưng có

quyền kiểm soát đối với các ứng dụng đã triển khai và có thể có quyền cấu hình môi trường lưu trữ/ khởi chạy ứng dụng.

c) Phần mềm dưới dạng dịch vụ (**SaaS** - Software as a Service): Sử dụng các ứng dụng của nhà cung cấp dịch vụ chạy trên hạ tầng đám mây. Các ứng dụng này có thể được truy cập từ nhiều thiết bị khác nhau thông qua trình duyệt web hoặc thông qua một số ứng dụng. Người dùng không quản lý hay kiểm soát hạ tầng đám mây bên dưới, bao gồm mạng, máy chủ, hệ điều hành, lưu trữ, hoặc thậm chí là các chức năng của ứng dụng; ngoại trừ một số thiết lập cấu hình ứng dụng giới hạn ở mức cá nhân hóa cho người dùng.

d) Chức năng dưới dạng dịch vụ (**FaaS** - Function as a Service): Phát triển, quản lý và vận hành các chức năng, ứng dụng mà không cần quản lý hạ tầng nào. Người dùng chỉ cần viết hàm (function) để xử lý sự kiện xảy ra (ví dụ: khi có yêu cầu HTTP, tải file lên, hay dữ liệu thay đổi) và hệ thống đám mây sẽ tự động chạy hàm đó, người dùng không tự xây dựng hay quản lý hạ tầng phức tạp bên dưới.

III. CÁC YÊU CẦU ĐẢM BẢO AN NINH MẠNG ĐỐI VỚI NỀN TẢNG ĐIỆN TOÁN Đám Mây Phục vụ CHÍNH PHỦ ĐIỆN TỬ/ CHÍNH QUYỀN ĐIỆN TỬ

3.1. Quản lý và kiểm soát tài sản phần cứng

Đáp ứng yêu cầu tại Mục 5.2 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý tài sản phần cứng.

3.2. Quản lý và kiểm soát tài sản phần mềm

Đáp ứng yêu cầu tại Mục 5.3 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý tài sản phần mềm.

3.3. Quản lý tài sản thông tin

Đáp ứng yêu cầu tại Mục 5.4 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý tài sản thông tin.

Ngoài ra, cơ quan và tổ chức cần đáp ứng bổ sung thêm yêu cầu sau:

3.3.1. Thiết lập cơ chế chia sẻ dữ liệu an toàn

a) Thiết lập các cơ chế kỹ thuật và chính sách đảm bảo dữ liệu được xác thực và định danh trước và trong quá trình truyền gửi.

b) Nhà cung cấp dịch vụ ĐTĐM chỉ chia sẻ dữ liệu của khách hàng sử dụng dịch vụ ĐTĐM với chính khách hàng đó hoặc các trường hợp khác theo quy định của pháp luật.

c) Nền tảng ĐTĐM đảm bảo không một bên thứ ba trái phép nào (áp dụng với cả nhà cung cấp dịch vụ ĐTĐM) có thể truy cập, thay đổi, phá hủy dữ liệu trong quá trình chia sẻ, yêu cầu:

- Nơi lưu trữ dữ liệu: có biện pháp kỹ thuật đảm bảo dữ liệu của CPĐT/CQĐT được lưu trữ trong lãnh thổ Việt Nam theo quy định.
- Quản lý khoá: Nhà cung cấp hỗ trợ các cơ chế cho phép khách hàng tự quản lý và kiểm soát hoàn toàn khoá mã hoá. Toàn bộ khoá mã hoá dùng cho dữ liệu của CPĐT/CQĐT phải được lưu trữ và quản lý bên trong lãnh thổ Việt Nam.
- Ghi nhật ký kiểm toán chi tiết, đầy đủ và bất biến cho mọi hoạt động truyền

3.3.2. Đảm bảo tính di động của dữ liệu và khả năng chuyển đổi nhà cung cấp

a) Nhà cung cấp dịch vụ ĐTĐM phải cung cấp công cụ hoặc giao diện lập trình ứng dụng (API) theo chuẩn mở, cho phép khách hàng trích xuất toàn bộ dữ liệu (bao gồm dữ liệu ứng dụng, cấu hình và siêu dữ liệu) một cách an toàn, toàn vẹn và có cấu trúc.

b) Hợp đồng cung cấp dịch vụ phải có điều khoản quy định rõ quy trình, trách nhiệm hỗ trợ của nhà cung cấp và chi phí (nếu có) khi khách hàng có nhu cầu chuyển đổi sang nền tảng ĐTĐM của nhà cung cấp khác.

3.4. Cấu hình an toàn cho phần cứng và phần mềm

a) Đáp ứng yêu cầu tại Mục 5.5 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Cấu hình an toàn cho phần cứng và phần mềm.

b) Nhà cung cấp dịch vụ ĐTĐM tăng cường thiết lập cấu hình bảo mật dịch vụ ảo hóa, bao gồm nhưng không giới hạn:

- Dịch vụ xác thực;
- Dịch vụ quản trị giao diện dashboard;
- Dịch vụ tính toán;
- Dịch vụ lưu trữ;
- File ảnh của máy ảo, máy chủ ảo, container;
- Dịch vụ chia sẻ lưu trữ;
- Dịch vụ quản lý mạng;
- Dịch vụ thanh toán.

c) Nhà cung cấp dịch vụ ĐTĐM có cơ chế bảo vệ các API bằng các biện pháp xác thực, kiểm soát truy cập, mã hóa dữ liệu, giới hạn tần suất truy cập phù hợp. Hoạt động truy cập vào API phải được ghi nhật ký đầy đủ và định kỳ rà soát 01 lần/ năm hoặc khi có thay đổi ảnh hưởng đến hệ thống.

3.5. Quản lý tài khoản và quyền truy cập tài khoản của người dùng

Đáp ứng yêu cầu tại Mục 5.6 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý tài khoản và quyền truy cập tài khoản của người dùng.

Ngoài ra, cơ quan và tổ chức cần đáp ứng bổ sung thêm yêu cầu sau:

3.5.1. Xây dựng và tuân thủ quy định quản lý truy cập của nhà cung cấp dịch vụ/bên thứ ba

a) Xây dựng, ban hành và đảm bảo tuân thủ quy định/ quy trình cấp quyền truy cập cho nhà cung cấp dịch vụ/ bên thứ ba.

b) Chỉ cấp quyền truy cập vào môi trường cho nhà cung cấp dịch vụ hoặc bên thứ ba khi có yêu cầu và được phê duyệt bởi người có thẩm quyền.

c) Quá trình truy cập phải được ghi nhật ký hệ thống và thu hồi quyền ngay sau khi hoàn tất công việc.

3.6. Quản lý lỗ hổng bảo mật

Đáp ứng yêu cầu tại Mục 5.7 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý lỗ hổng bảo mật.

3.6.1. Tìm kiếm chủ động mối đe dọa

Cơ quan, tổ chức và nhà cung cấp dịch vụ ĐTĐM thực hiện tìm kiếm chủ động mối đe dọa đối với hệ thống, máy chủ.

3.7. Quản lý nhật ký an ninh mạng

Đáp ứng yêu cầu tại Mục 5.8 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý nhật ký an ninh mạng.

3.8. Bảo vệ cho trình duyệt web, dịch vụ thư điện tử

Đáp ứng yêu cầu tại Mục 5.9 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Bảo vệ cho trình duyệt web, dịch vụ thư điện tử.

3.9. Phòng chống phần mềm độc hại

Đáp ứng yêu cầu tại Mục 5.10 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Phòng chống phần mềm độc hại.

3.10. Sao lưu và khôi phục dữ liệu

Đáp ứng yêu cầu tại Mục 5.11 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Sao lưu và khôi phục dữ liệu.

3.11. Quản lý hạ tầng mạng

Đáp ứng yêu cầu tại Mục 5.12 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý hạ tầng mạng.

Ngoài ra, cơ quan, tổ chức và nhà cung cấp dịch vụ ĐTĐM cần đáp ứng bổ sung yêu cầu sau:

3.11.1. Xây dựng và áp dụng quy trình quản lý thay đổi

Xây dựng, ban hành và đảm bảo tuân thủ quy trình quản lý thay đổi. Định kỳ rà soát 01 lần/ năm hoặc khi có thay đổi ảnh hưởng đến quy trình. Đáp ứng tối thiểu các yêu cầu sau:

- Thông báo cho các bên có thể bị ảnh hưởng về sự thay đổi;
- Trước khi triển khai bất kỳ thay đổi nào trong môi trường hoạt động, phải thực hiện đánh giá các tác động liên quan đến an ninh mạng và khả năng tương thích của phần mềm đối với hệ thống, nền tảng và các thành phần khác có liên quan; đồng thời, thông báo đầy đủ cho khách hàng sử dụng dịch vụ bị ảnh hưởng và bên thứ ba liên quan về nội dung, phạm vi thay đổi.
- Nhà cung cấp dịch vụ ĐTĐM thực hiện sao lưu dữ liệu các hệ thống hoặc ứng dụng bị ảnh hưởng trước khi triển khai thay đổi, trừ trường hợp thay đổi đó đã được kiểm tra đầy đủ trong môi trường tương đương với môi trường hoạt động.
- Khi gặp vấn đề trong hoặc sau thực hiện thay đổi cần đảm bảo hệ thống có thể khôi phục lại phiên bản trước khi thay đổi được triển khai. Trường hợp không thể quay về phiên bản trước phải xác định và chuẩn bị các phương án phục hồi thay thế phù hợp.
- Tiến hành đánh giá rủi ro trước, trong và sau khi thay đổi.

3.11.2. Xây dựng và áp dụng chính sách quản lý truy cập vào trình ảo hóa hypervisor

a) Trong quản lý truy cập từ xa vào trình ảo hóa hypervisor, đảm bảo tuân thủ tiêu chí 3.5 về Quản lý tài khoản và quyền truy cập tài khoản của người dùng; đảm bảo tuân thủ tiêu chí 5.12.2.5 trong TCVN 14423:2025 về Xây dựng và áp dụng chính sách quản lý truy cập từ xa.

b) Xây dựng quy trình yêu cầu truy cập từ xa và phải được người có thẩm quyền phê duyệt đúng chức năng nhiệm vụ, đúng yêu cầu.

3.11.3. Quản lý bảo mật cho IaC

a) Các tệp mã nguồn IaC phải được lưu trữ và quản lý trong hệ thống quản lý mã nguồn có khả năng kiểm soát phiên bản và truy vết đầy đủ. Chỉ những cá nhân được ủy quyền mới được phép truy cập, chỉnh sửa hoặc triển khai các tệp IaC.

b) Nhà cung cấp dịch vụ ĐTĐM có trách nhiệm tích hợp công cụ quét bảo mật mã nguồn tĩnh cho các tệp IaC, việc quét bảo mật phải được thực hiện tự động trước khi triển khai.

c) Không lưu trữ thông tin nhạy cảm dưới dạng rõ trong các tệp IaC hoặc hệ thống quản lý mã nguồn.

d) Các tệp cấu hình IaC phải được kiểm thử trong môi trường thử nghiệm độc lập trước khi đưa vào triển khai chính thức. Nhà cung cấp phải có phương án đảm bảo tài nguyên được triển khai từ IaC đáp ứng đầy đủ các yêu cầu bảo mật và tuân thủ chính sách nội bộ.

3.12. Giám sát và phòng thủ an ninh mạng

a) Đáp ứng yêu cầu tại Mục 5.13 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Giám sát và phòng thủ an ninh mạng.

b) Giải pháp giám sát cho nền tảng điện toán đám mây phục vụ CPĐT/CQĐT phải có khả năng kết nối, chia sẻ dữ liệu giám sát về hệ thống giám sát của Trung tâm An ninh mạng quốc gia, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

3.13. Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

Đáp ứng yêu cầu tại Mục 5.14 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng.

Ngoài ra, cơ quan và tổ chức cần đáp ứng bổ sung thêm yêu cầu sau:

3.13.1. Xác minh lý lịch cho nhân sự chuyên trách/ kiêm nhiệm quản trị hệ thống ĐTĐM

a) Có cơ chế xác minh lý lịch nhân sự và đánh giá liên tục đối với cán bộ chuyên trách/ kiêm nhiệm quản trị hệ thống ĐTĐM.

b) Nhà cung cấp dịch vụ điện toán đám mây sử dụng nhân sự vận hành là người nước ngoài phải tuân thủ theo quy định pháp luật hiện hành. Có cơ chế bảo lãnh, xác minh lý lịch, cam kết bảo mật trong quá trình làm việc.

3.14. Quản lý nhà cung cấp dịch vụ

Đáp ứng yêu cầu tại Mục 5.15 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý nhà cung cấp sản phẩm, dịch vụ.

Ngoài ra, cơ quan, tổ chức và nhà cung cấp dịch vụ ĐTĐM cần đáp ứng bổ sung yêu cầu sau:

3.14.1. Thiết lập, duy trì định danh nhà cung cấp dịch vụ

Xây dựng, ban hành và đảm bảo tuân thủ quy định định danh đối với các nhà cung cấp dịch vụ ĐTĐM phục vụ CPĐT/CQĐT, tối thiểu bao gồm:

- Đáp ứng yêu cầu pháp lý theo quy định hiện hành;
- Định danh điện tử doanh nghiệp;
- Có đại diện pháp lý, chi nhánh hoặc văn phòng đại diện tại Việt Nam;
- Đặt hạ tầng vật lý hoặc trung tâm dữ liệu tại Việt Nam

3.14.2. Đảm bảo an toàn trong thỏa thuận với nhà cung cấp dịch vụ

a) Nhà cung cấp dịch vụ thực hiện xây dựng, ban hành và đảm bảo tuân thủ quy trình hủy bỏ dữ liệu triệt để. Định kỳ rà soát tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy trình.

Nhà cung cấp dịch vụ có phương án/ biện pháp kỹ thuật đảm bảo dữ liệu đã được hủy bỏ một cách an toàn và không thể khôi phục được thể hiện trong hợp đồng.

b) Đảm bảo hợp đồng nhà cung cấp dịch vụ ĐTĐM và khách hàng đáp ứng đầy đủ yêu cầu tối thiểu: yêu cầu về bảo đảm an ninh mạng cho hệ thống ĐTĐM; năng lực vận hành và quản trị ĐTĐM; thông tin định danh cá nhân; kết nối giám sát và chia sẻ thông tin sự cố an ninh mạng về Trung tâm An ninh mạng quốc gia, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

c) Khi nhà cung cấp dịch vụ ĐTĐM sử dụng dịch vụ của các nhà cung cấp dịch vụ ĐTĐM ngang hàng, nhà cung cấp có trách nhiệm đảm bảo độ tin cậy và mức độ an toàn thông tin đối với khách hàng không thấp hơn mức độ được duy trì trong trường hợp không sử dụng các dịch vụ ĐTĐM bên thứ ba.

d) Nhà cung cấp dịch vụ xác định mục tiêu an ninh mạng và yêu cầu các bên trong chuỗi cung ứng thực hiện đầy đủ các biện pháp quản lý rủi ro để đáp ứng mục tiêu đã đề ra.

3.15. Phát triển ứng dụng an toàn

Đáp ứng yêu cầu tại Mục 5.16 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Phát triển ứng dụng an toàn.

3.16. Quản lý ứng phó sự cố an ninh mạng

a) Đáp ứng yêu cầu tại Mục 5.17 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản trị ứng phó sự cố an ninh mạng.

b) Nhà cung cấp dịch vụ ĐTĐM xây dựng, ban hành quy định ứng phó sự cố an ninh mạng, tối thiểu bao gồm:

- Xác định phạm vi của sự cố an ninh mạng được phát hiện;
- Quy trình báo cáo sự cố an ninh mạng;
- Thiết lập kênh liên lạc an toàn phục vụ các vấn đề liên quan đến sự cố an ninh mạng;
- Cơ chế phối hợp với khách hàng sử dụng dịch vụ ĐTĐM và cơ quan chức năng trong điều phối, ứng phó sự cố.

Nhà cung cấp dịch vụ ĐTĐM thực hiện chia sẻ thông tin, báo cáo sự cố trong vòng 24h kể từ khi phát hiện về Trung tâm An ninh mạng quốc gia, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an để phối hợp điều phối, ứng phó sự cố.

c) Nhà cung cấp dịch vụ ĐTĐM xây dựng phương án ứng cứu sự cố; phương án đảm bảo hệ thống, dịch vụ ĐTĐM hoạt động liên tục; phương án khôi phục sau thảm họa; thực hiện thử nghiệm các phương án để bảo đảm tính sẵn sàng của nền tảng ĐTĐM. Đánh giá và cập nhật phương án tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi ảnh hưởng đến phương án.

3.17. Quản lý kiểm tra an ninh mạng

a) Đáp ứng yêu cầu tại Mục 5.18 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý kiểm tra an ninh mạng.

b) Nhà cung cấp dịch vụ ĐTĐM thực hiện đánh giá, kiểm thử an ninh mạng để đảm bảo an toàn cho hệ thống. Hệ thống ĐTĐM phải được kiểm tra, đánh giá an ninh mạng theo quy định của pháp luật.

c) Việc kiểm tra, đánh giá an ninh mạng phải do cơ quan chức năng thực hiện theo quy định của pháp luật.

3.18. Quản lý rủi ro an ninh mạng

a) Đáp ứng yêu cầu tại Mục 5.1 của TCVN 14423:2025 (áp dụng với cả các hệ thống và dịch vụ ảo hóa) về Quản lý rủi ro an ninh mạng.

b) Đánh giá rủi ro an ninh mạng cho hệ thống ĐTĐM tối thiểu phải bao gồm các rủi ro liên quan đến Quản trị đám mây; An ninh hạ tầng đám mây; Quản lý hoạt động đám mây; Quản lý dịch vụ đám mây; Truy cập khách hàng dịch vụ đám mây;

Tách biệt giữa các khách hàng dịch vụ điện toán đám mây (bao gồm các rủi ro an ninh do ảo hóa); Phần mềm mã nguồn mở hoặc vendor lock-in và bất kỳ sự thay đổi ảnh hưởng đến tổ chức.

c) Định kỳ (tối thiểu 01 lần/ 01 năm) đánh giá rủi ro của nhà cung cấp dịch vụ ĐTĐM do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được các cấp có thẩm quyền chỉ định thực hiện.

3.19. Quản lý an toàn vật lý

Chỉ cấp quyền truy cập vật lý tạm thời cho khách hàng khi được ủy quyền hoặc được sự đồng ý của người có thẩm quyền trong cơ quan, tổ chức. Trong quá trình khách hàng truy cập, nhà cung cấp dịch vụ ĐTĐM/cơ quan, tổ chức sử dụng dịch vụ ĐTĐM phải có nhân sự giám sát; ghi nhận đầy đủ quá trình truy cập; thu hồi quyền truy cập ngay sau khi hết nhiệm vụ và định kỳ (tối thiểu 01 lần/ 01 quý) rà soát nhật ký khách tham quan./.