

THUYẾT MINH DỰ THẢO TIÊU CHUẨN QUỐC GIA

AN NINH MẠNG - NỀN TẢNG TÍNH TOÁN Đám Mây PHỤC VỤ HẠ TẦNG SỐ TRỌNG YẾU - YÊU CẦU CHUNG

1. Thông tin chung về dự thảo TCVN

a) Tên dự thảo TCVN

TCVN XXXXX:2026, An ninh mạng - Nền tảng tính toán đám mây phục vụ hạ tầng số trọng yếu - Yêu cầu chung.

b) Thuộc lĩnh vực

Tiêu chuẩn thuộc lĩnh vực tiêu chuẩn cho sản phẩm, dịch vụ an ninh mạng.

c) Phạm vi áp dụng của TCVN

Tiêu chuẩn này quy định các yêu cầu kỹ thuật chung đối với nền tảng tính toán đám mây phục vụ hạ tầng số trọng yếu.

d) Mục tiêu của TCVN

Tạo lập một hệ quy chiếu đo lường và kiểm định kỹ thuật thống nhất, làm căn cứ pháp lý độc lập cho công tác đánh giá, cấp chứng nhận hợp chuẩn sản phẩm trước khi đưa vào lưu hành. Tiêu chuẩn sẽ đóng vai trò là thước đo kỹ thuật bắt buộc để các cơ quan nhà nước và chủ quản hệ thống thông tin trọng yếu tham chiếu trong quá trình thiết kế kiến trúc, lập hồ sơ thầu và nghiệm thu các nền tảng tính toán đám mây. Đồng thời, đây cũng là định hướng cho các doanh nghiệp công nghệ trong nước chuẩn hóa kiến trúc đám mây an toàn, tạo đòn bẩy thúc đẩy quá trình nghiên cứu, phát triển nền tảng đám mây "Make in Vietnam" đạt chất lượng tương đương quốc tế và đáp ứng toàn diện yêu cầu bảo vệ chủ quyền công nghệ, chủ quyền dữ liệu trên không gian mạng.

đ) Cơ quan chủ trì soạn thảo

- Tên cơ quan: Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an.

- Địa chỉ: Lô E2, khu đô thị mới Cầu Giấy, Phường Cầu Giấy, Thành phố Hà Nội.

e) Tổ chức tham gia soạn thảo

Tham gia soạn thảo tiêu chuẩn quốc gia (TCVN) này bao gồm: Các cán bộ Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; Cục Khoa học, Chiến lược và Lịch sử Công an; Các chuyên gia về điện toán đám mây và an ninh mạng.

g) Phiên bản dự thảo: Version 1

2. Nội dung dự thảo TCVN

DỰ THẢO TCVN	THUYẾT MINH
1. Phạm vi áp dụng	Ban biên soạn tự xây dựng.
2. Tài liệu viện dẫn	Tham khảo các tiêu chuẩn quốc gia hiện hành (TCVN 14423:2026, TCVN 12480:2019, TCVN 12481:2019, v.v.) và các văn bản quy phạm pháp luật liên quan (Luật An ninh mạng, Luật Bảo vệ dữ liệu cá nhân).
3. Thuật ngữ, định nghĩa và chữ viết tắt	Tự xây dựng. Cụ thể hóa các định nghĩa đặc thù về đám mây như Khách hàng dịch vụ tính toán đám mây (CSC), Infrastructure as Code (IaC), Vendor lock-in, Hypervisor, Mô hình chia sẻ trách nhiệm.
4. Nguyên tắc áp dụng và mô hình chia sẻ trách nhiệm	Tự xây dựng dựa trên nguyên tắc thực tiễn vận hành đám mây đa tiền thuê.
4.1 Nguyên tắc áp dụng	Tự xây dựng. Phân định rõ tiêu chuẩn áp dụng cho nền tảng, không áp dụng cho ứng dụng nội bộ của chủ thuê.
4.2 Mức áp dụng, mô hình tin cậy và điều kiện tiên quyết	Tự xây dựng. Xác định 3 mức độ (Mức 3, Mức 4, Mức 5) tương ứng với cấp độ hệ thống thông tin theo quy định và áp dụng kiến trúc Zero-Trust đối với Mức 5.
4.3 Phân định và chia sẻ trách nhiệm	Tự xây dựng. Yêu cầu làm rõ trách nhiệm giữa CSP và CSC để không tồn tại khoảng trống an ninh.
4.4 Trách nhiệm đối với chuỗi cung ứng dịch vụ	Ban biên soạn tự xây dựng, ràng buộc các yêu cầu bảo mật với bên thứ ba không thấp hơn cam kết với chủ thuê.
5. Quản trị an ninh mạng và quản lý rủi ro	Tự xây dựng trên cơ sở tham chiếu TCVN 14423:2026.
5.1 Khái quát	Tự xây dựng.
5.2 Yêu cầu cụ thể	Tham khảo TCVN 14423:2026 về quản

	trì an ninh mạng và bổ sung quản lý rủi ro rò rỉ dữ liệu, cạn kiệt tài nguyên trong môi trường đám mây dùng chung.
6. Yêu cầu an toàn chung đối với nền tảng	Tự xây dựng dựa trên kiến trúc tham chiếu đám mây.
6.1 Khái quát	Tự xây dựng. Thiết lập yêu cầu kỹ thuật lõi bảo vệ hệ thống trước rủi ro môi trường đa tiền thuê.
6.2 Yêu cầu cụ thể	Tự xây dựng và tham khảo các tiêu chuẩn quốc tế về an toàn đám mây.
6.2.1 Kiến trúc an toàn, phân tách thuê bao và bảo vệ mặt phẳng điều khiển	Tự xây dựng, bao gồm yêu cầu độc lập phân hệ, phân tách ở lớp ảo hóa, toàn vẹn khởi động, chứng thư số và khả năng chịu lỗi.
6.2.2 Bảo vệ mạng và kết nối an toàn	Ban biên soạn tự xây dựng, tập trung phân lập mạng VPC, tường lửa phân tán, mã hóa đường truyền và định tuyến an toàn.
6.2.3 Quản lý danh tính, quyền truy cập và đặc quyền	Ban biên soạn tự xây dựng, bao gồm cơ chế RBAC, xác thực liên tục theo ngữ cảnh và phân tách/mở quyền khẩn cấp có thời hạn.
6.2.4 Bảo vệ dữ liệu, mật mã và quản lý khóa	Tham khảo quy định pháp luật về cơ yếu, yêu cầu HSM, xóa dữ liệu an toàn và linh hoạt thay thế thuật toán mã hóa (kháng lượng tử).
6.2.5 Quản lý cấu hình, điểm yếu, thay đổi và sự cố	Tự xây dựng, quy định về di chuyển máy ảo, quản lý IaC, vá khẩn cấp, cảnh báo sự cố có giới hạn phạm vi rò rỉ thông tin.
6.2.6 Nhật ký, giám sát, tích hợp và cung cấp bằng chứng	Tham khảo TCVN 13054-1:2020. Yêu cầu nhật ký bất biến, neo toàn vẹn mật mã và trích xuất chứng cứ số cho chủ thuê.
6.2.7 Sao lưu, phục hồi, tính liên tục và triển khai đa vùng	Tự xây dựng, bắt buộc sao lưu bất biến, diễn tập khôi phục thảm họa (DR) và luân chuyển tải đa vùng tự động.
6.2.8 Quản lý chuỗi cung ứng, khả chuyển và chủ quyền công nghệ	Tự xây dựng, đặt ra tiêu chuẩn cao về làm chủ mã nguồn lõi tại Việt Nam, vận hành ngoại tuyến và sinh SBOM tự động.
7. Yêu cầu chức năng nghiệp vụ riêng đối với sản phẩm theo mô	Ban biên soạn tự xây dựng dựa trên các mô hình dịch vụ đám mây đặc thù.

hình dịch vụ	
7.1 Khái quát	Tự xây dựng.
7.2 Yêu cầu cụ thể	Tự xây dựng.
7.2.1 Yêu cầu riêng đối với mô hình dịch vụ hạ tầng (IaaS)	Cụ thể hóa các tính năng công tự phục vụ, cấu hình VPC, tải ảnh hệ điều hành (BYOI) và giám sát tiêu thụ tài nguyên.
7.2.2 Yêu cầu riêng đối với mô hình dịch vụ nền tảng (PaaS)	Cụ thể hóa tự động hóa cài đặt, mở rộng quy mô, CI/CD và trích xuất nhật ký ứng dụng tập trung.
7.2.3 Yêu cầu riêng đối với mô hình dịch vụ phần mềm (SaaS)	Cụ thể hóa kiến trúc cách ly dữ liệu logic, hỗ trợ đăng nhập một lần (SSO) và khả năng chuyển dữ liệu nghiệp vụ ra định dạng mở.
Phụ lục A (quy định) Bảng áp dụng yêu cầu theo mức	Tổng hợp yêu cầu bắt buộc và khuyến nghị theo từng Mức (3, 4, 5) để thuận tiện tra cứu.
Phụ lục B (quy định) Phương pháp thử nghiệm	Tự xây dựng hệ thống 21 kịch bản thử nghiệm đánh giá độc lập (VD: cách ly mạng, Red Teaming, tính bất biến của bản sao lưu).
Phụ lục C (quy định) Bảng ánh xạ sang TCVN 14423:2026 và danh mục mối đe dọa, lỗ hổng	Tự xây dựng, giúp đối chiếu các yêu cầu an toàn đám mây với chuẩn hệ thống thông tin cơ bản.
Phụ lục D (tham khảo) Hướng dẫn xây dựng lộ trình chuyển đổi mật mã kháng lượng tử	Tự xây dựng lộ trình 5 giai đoạn nhằm chuẩn bị nền tảng trước nguy cơ từ máy tính lượng tử trong tương lai.