LIÊN HIỆP CÁC HỘI KHOA HỌC VÀ KỸ THUẬT VIỆT NAM
VIỆN KINH TẾ, PHÁP LUẬT VÀ QUẢN LÝ

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

Số: 059/CV-VKTPL&QL/2025

TP.HCM, ngày 25 tháng 06 năm 2026

VĂN PHÒNG UBND TỈNH ĐẮK LẮK
ĐẾN Số: 16534
Ngày: 29/6/2026
Chuyển:

THƯ ĐỀ XUẤT

(V/v: Phối hợp nghiên cứu triển khai các chương trình hợp tác về lĩnh vực khoa học công nghệ, xây dựng các chiến lược phát triển kinh tế và đầu tư)

Kính gửi: **- UBND TỈNH ĐẮK LẮK**
- Bà HỒ THỊ NGUYÊN THẢO – PCT TT UBND TỈNH ĐẮK LẮK

Viện Kinh tế, Pháp luật và Quản Lý (sau đây gọi tắt là Viện) là một đơn vị trực thuộc của Liên Hiệp Các Hội Khoa Học và Kỹ thuật Việt Nam thành viên của Trung Ương Mặt Trận Tổ Quốc Việt Nam, Viện được Bộ Khoa Học và Công Nghệ cấp giấy phép hoạt động từ năm 2017.

Viện là một đơn vị có nhiều năm kinh nghiệm hoạt động trong lĩnh vực nghiên cứu khoa học, đưa ra các báo cáo, các giải pháp toàn diện và phối hợp triển khai các chiến lược tổng thể trong các lĩnh vực khoa học công nghệ, xây dựng các chiến lược phát triển kinh tế và đầu tư.

***Căn cứ vào*:**

- *Nghị quyết số 57-NQ/TW của Bộ Chính trị,*
- *Quyết định số 569/QĐ-TTg của Thủ tướng Chính phủ,*
- *Kế hoạch số 092/KH-UBND về việc phát triển khoa học, công nghệ và đổi mới sáng tạo tỉnh Đắk Lắk giai đoạn 2026-2030,*
- *Kế hoạch 160/KH-UBND của Ủy ban nhân dân tỉnh Đắk Lắk đánh giá hoạt động khoa học, công nghệ và đổi mới sáng tạo năm 2026 trên địa bàn tỉnh Đắk Lắk*

Viện xin trân trọng gửi đến UBND Tỉnh Đắk Lắk đề án đề xuất **"Chiến lược tổng thể bảo đảm an toàn thông tin, bảo vệ dữ liệu và phát triển hạ tầng số tỉnh Đắk Lắk giai đoạn 2026-2030 tầm nhìn 2035"** *(hồ sơ đính kèm).*

Chúng tôi rất mong sớm nhận được sự phản hồi của UBND Tỉnh Đắk Lắk để có thể tiếp tục triển khai các bước tiếp theo với các Sở, Ban, Ngành và Chính quyền địa phương cấp xã, phường của Tỉnh.

Mọi thông tin phản hồi xin vui lòng liên lạc hoặc gửi về:

VIỆN KINH TẾ, PHÁP LUẬT VÀ QUẢN LÝ
Người nhận: **TS. Phan Ngọc Dũng (0909060392)**
Email: Vientruong@vkt-gov.com
Địa chỉ: Tòa nhà VP, 781/C2 Lê Hồng Phong, Phường Hòa Hưng, Tp.HCM

Xin chân thành cảm ơn và trân trọng kính chào!

VIỆN KINH TẾ, PHÁP LUẬT VÀ QUẢN LÝ
Viện Trưởng kiêm CT Hội đồng khoa học

TS. PHAN NGỌC DŨNG

VIỆN KINH TẾ, PHÁP LUẬT VÀ QUẢN LÝ

***

Đề án Đề xuất

CHIẾN LƯỢC TỔNG THỂ BẢO ĐẢM AN TOÀN THÔNG TIN, BẢO VỆ DỮ LIỆU VÀ PHÁT TRIỂN HẠ TẦNG SỐ TỈNH ĐẮK LẮK GIAI ĐOẠN 2026 - 2030, TẦM NHÌN 2035

Cơ quan đề xuất:	Viện Kinh tế, Pháp luật và Quản lý
Cơ quan tiếp nhận:	Ủy ban Nhân dân tỉnh Đắk Lắk

Kính gửi: Ủy ban Nhân dân tỉnh Đắk Lắk.

Căn cứ vào chức năng, nhiệm vụ nghiên cứu và tư vấn chiến lược của Viện Kinh tế, Pháp luật và Quản lý; căn cứ vào nhu cầu thực tiễn của địa phương trong công cuộc chuyển đổi số, Viện Kinh tế, Pháp luật và Quản lý trân trọng đệ trình Đề án "Chiến lược tổng thể bảo đảm an toàn thông tin, bảo vệ dữ liệu và phát triển hạ tầng số tỉnh Đắk Lắk giai đoạn 2026 - 2030, tầm nhìn 2035" với các nội dung trọng tâm như sau:

I. CĂN CỨ XÂY DỰNG ĐỀ ÁN VÀ BỐI CẢNH CHIẾN LƯỢC:

1. Phân tích nền tảng pháp lý tối cao và hành lang quản trị an ninh mạng

Đề án quy hoạch chiến lược an toàn thông tin (ATTT) và bảo vệ dữ liệu của tỉnh Đắk Lắk được xây dựng trên một nền tảng pháp lý đang có những bước chuyển mình mang tính bước ngoặt, chuyển trọng tâm từ việc đơn thuần bảo vệ hệ thống vật lý sang việc quản trị vòng đời và bảo vệ quyền cơ bản của công dân đối với dữ liệu cá nhân. Nền tảng này bắt đầu từ Luật An toàn thông tin mạng số 86/2015/QH13 và Luật An ninh mạng số 24/2018/QH14, thiết lập các quy chuẩn tối cao về bảo vệ hệ thống thông tin quan trọng liên quan đến an ninh quốc gia. Các văn bản này quy định rõ trách nhiệm của cơ quan chủ quản trong việc thiết lập các phương án bảo vệ đa lớp, đồng thời tạo ra hành lang pháp lý để lực lượng chuyên trách tiến hành các biện pháp nghiệp vụ phòng ngừa, đấu tranh với tội phạm công nghệ cao.

Đặc biệt, sự ra đời của Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, được Quốc hội thông qua và chính thức có hiệu lực từ ngày 01/01/2026, đã định hình lại toàn bộ cấu trúc quản trị dữ liệu số của quốc gia. Đạo luật này không chỉ thay thế các quy định rải rác trước đây mà còn luật hóa toàn diện Nghị định 13/2023/NĐ-CP, đặt ra các tiêu chuẩn khắt khe về trách nhiệm giải trình của bên kiểm soát và xử lý dữ liệu. Đi kèm với Luật là Nghị định số 356/2025/NĐ-CP quy định chi tiết việc thi hành, tạo ra một cơ chế giám sát thực thi cực kỳ nghiêm ngặt. Theo Nghị định 356/2025/NĐ-CP, các cơ quan, tổ chức bắt buộc phải thiết lập hệ thống Đánh giá tác động xử lý dữ liệu (PIA), quản lý quyền chủ thể dữ liệu (DSR), và đối mặt với các chế tài xử phạt mang tính răn đe cực cao. Cụ thể, các vi phạm liên quan đến chuyển dữ liệu xuyên biên giới trái phép hoặc mua bán dữ liệu có thể bị phạt từ 5% đến 10% tổng doanh thu, hoặc lên tới 3 tỷ đồng. Điều này đặt ra áp lực tuân thủ khổng lồ lên bộ máy chính quyền các cấp cũng như cộng đồng doanh nghiệp đóng trên địa bàn.

Bên cạnh đó, việc thực thi Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ tiếp tục được đẩy mạnh thông qua Chỉ thị 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ. Chỉ thị này yêu cầu sự quyết liệt từ người đứng đầu các cấp trong việc hoàn thành hồ sơ đề xuất và triển khai phương án bảo đảm ATTT theo

cấp độ. Đồng thời, việc thực hiện Đề án 06/CP về phát triển ứng dụng dữ liệu dân cư, định danh và xác thực điện tử giai đoạn 2022-2025, tầm nhìn 2030 đang tạo ra một khối lượng dữ liệu khổng lồ, hội tụ về một mối, đòi hỏi các địa phương phải có năng lực bảo mật ở mức độ quốc gia để ngăn chặn các nguy cơ lộ lọt từ bên trong lẫn bên ngoài.

2. Bối cảnh quốc gia và bức tranh chuyển đổi số tại địa phương (Tỉnh Đắk Lắk)

Trên bình diện quốc gia, công cuộc chuyển đổi số đã bước qua giai đoạn "số hóa thủ tục" để tiến vào kỷ nguyên "dữ liệu hóa" và "trí tuệ nhân tạo". Sự hội tụ của công nghệ mạng di động thế hệ thứ 5 (5G), Internet vạn vật (IoT), và điện toán đám mây (Cloud Computing) đang mang lại những giá trị thặng dư to lớn cho nền kinh tế, nhưng đồng thời cũng mở rộng bề mặt tấn công (attack surface) theo cấp số nhân. Trong bối cảnh đó, tỉnh Đắk Lắk đã thể hiện quyết tâm chính trị mạnh mẽ, đưa chuyển đổi số trở thành động lực nội sinh cho sự phát triển kinh tế - xã hội. Kết quả phản ánh qua Chỉ số đánh giá mức độ chuyển đổi số (DTI) năm 2024, tỉnh Đắk Lắk đứng thứ 29/34 tỉnh, thành phố trực thuộc Trung ương. Phân tích sâu hơn vào các trụ cột, tỉnh xếp hạng 29 về chính quyền số, 28 về kinh tế số và 28 về xã hội số. Ở cấp cơ sở, Sở Nông nghiệp và Phát triển nông thôn cùng UBND thành phố Buôn Ma Thuột đang là những đơn vị dẫn đầu về DTI nội tỉnh, cho thấy sự chênh lệch năng lực số giữa các ban ngành và các khu vực địa lý.

Tuy nhiên, quá trình vươn lên này đi kèm với những thách thức to lớn về hạ tầng vật lý và sự ổn định của hệ thống. Một minh chứng điển hình là thiệt hại do thiên tai gây ra đối với hạ tầng CNTT tại các Trung tâm Phục vụ hành chính công tuyến xã phía Đông (như Tuy An Nam, Đông Hòa, Hòa Xuân) vào tháng 11/2025. Đợt ngập lụt đã làm hư hỏng hàng loạt thiết bị số hóa, máy tính, thiết bị mạng với tổng thiệt hại gần 1,5 tỷ đồng. Nghiêm trọng hơn cả thiệt hại vật chất là rủi ro về an toàn định danh khi các Chứng thư số và chữ ký số do Ban Cơ yếu Chính phủ cấp cho cán bộ xã bị cuốn trôi và hư hỏng, dẫn đến việc giải quyết thủ tục hành chính bị đình trệ nghiêm trọng. Sự kiện này là hồi chuông cảnh báo về rủi ro vật lý đe dọa tính sẵn sàng (Availability) của hệ thống, đòi hỏi Đề án phải tích hợp tư duy phục hồi thảm họa (Disaster Recovery) ngay từ tuyến cơ sở.

Song song với khối chính quyền, bức tranh chuyển đổi số của khối doanh nghiệp công nghiệp trên địa bàn cũng đang có những bước tiến vượt bậc. UBND tỉnh đã ban hành Kế hoạch số 074/KH-UBND nhằm đẩy mạnh triển khai hạ tầng 5G và IoT tại 07 khu công nghiệp và 22 cụm công nghiệp. Đặc biệt, Khu công nghiệp Hòa Phú đang được đề xuất mở rộng thêm 150 ha để đáp ứng nhu cầu chế biến sâu nông sản xuất khẩu. Tỉnh đặt mục tiêu nâng tổng số trạm 5G lên 946 trạm (chiếm 20,9% tổng số trạm BTS) trong năm 2025, tạo nền tảng cho các ứng dụng giám sát môi trường và quản lý dây chuyền tự động hóa (SCADA/OT). Sự giao thoa giữa mạng công nghệ thông tin truyền thống (IT) và mạng công nghệ vận hành (OT) tại các KCN này tạo ra một hệ sinh thái kết nối khổng lồ, nhưng

cũng đồng thời tạo ra vô số điểm yếu bảo mật nếu không có một kiến trúc an ninh dùng chung (Security Architecture Framework) được quy chuẩn hóa ngay từ đầu.

3. Xu hướng rủi ro hệ thống, nguy cơ lộ lọt dữ liệu và các mối đe dọa tiên tiến:

Dựa trên các báo cáo phân tích mối đe dọa toàn cầu và đặc thù hạ tầng của Đắk Lắk, Viện Kinh tế, Pháp luật và Quản lý nhận diện 04 xu hướng rủi ro cốt lõi đang trực tiếp đe dọa đến nền tảng số của địa phương:

+ **Thứ nhất, sự gia tăng của các chiến dịch tấn công có chủ đích (APT) và mã độc tống tiền (Ransomware) thế hệ mới:** Tội phạm mạng hiện đại không còn tiến hành các cuộc tấn công rải thảm thiếu định hướng, mà chúng sử dụng Trí tuệ nhân tạo (AI) để tự động rà quét lỗ hổng, xâm nhập tĩnh lặng vào các trung tâm dữ liệu trọng yếu, nằm vùng nhiều tháng để trích xuất dữ liệu trước khi tiến hành mã hóa toàn bộ hệ thống. Đối với hệ thống bộ máy nhà nước, một cuộc tấn công Ransomware không chỉ gây thiệt hại về việc mất khả năng điều hành mà còn tạo ra sự khủng hoảng niềm tin nghiêm trọng từ phía người dân.

+ **Thứ hai, nguy cơ thất thoát dữ liệu (Data Leakage) nội bộ và rủi ro từ yếu tố con người:** Dữ liệu công dân không còn nằm im trong các máy chủ đóng kín mà liên tục luân chuyển qua thiết bị đầu cuối (máy trạm, điện thoại), qua các kênh mạng (email, web), và các nền tảng đám mây. Theo thống kê chuyên ngành, có tới 60% các vụ vi phạm dữ liệu xuất phát từ sự bất cẩn hoặc thiếu nhận thức của nhân sự nội bộ. Trong bối cảnh Luật Bảo vệ dữ liệu cá nhân 2025 yêu cầu kiểm soát chặt chẽ luồng dữ liệu, việc một nhân viên sao chép danh sách công dân ra ổ cứng USB cá nhân hoặc gửi nhầm qua ứng dụng chat không mã hóa cũng đủ để cấu thành hành vi vi phạm pháp luật nghiêm trọng.

+ **Thứ ba, sự mong manh của môi trường hội tụ IT-OT và IoT:** Kế hoạch phủ sóng 5G và triển khai hàng ngàn thiết bị cảm biến IoT tại các khu vực như KCN Hòa Phú mang lại lợi ích tự động hóa, nhưng các thiết bị IoT thường có năng lực bảo mật nội tại ở mức tương đối. Hacker có thể lợi dụng một camera an ninh hoặc cảm biến nhiệt độ bị lỗi phần mềm để xâm nhập vào mạng nội bộ của nhà máy, từ đó kiểm soát dây chuyền sản xuất hoặc đánh cắp bí mật thương mại, làm đứt gãy chuỗi cung ứng sản xuất hàng hóa của toàn tỉnh.

+ **Thứ tư, rủi ro đánh cắp danh tính và lạm dụng đặc quyền quản trị:** Việc quản lý tài khoản quản trị (Admin) tại các sở ban ngành thường diễn ra phân tán. Kỹ thuật viên từ các nhà thầu bên ngoài (vendors) khi tiến hành bảo trì thường được cấp quyền truy cập mức cao nhất mà không có cơ chế giám sát luồng thao tác. Điều này dẫn đến nguy cơ hình thành các "đặc quyền bóng tối" (Shadow Privileges) – nơi kẻ gian có thể sử dụng tài khoản hợp lệ để truy cập và can thiệp trực tiếp vào lõi cơ sở dữ liệu (Database) mà các hệ thống

tường lửa vòng ngoài không thể phát hiện.

II. ĐÁNH GIÁ HIỆN TRẠNG QUẢN TRỊ AN TOÀN THÔNG TIN TỈNH ĐẮK LẮK

1. Phân tích năng lực hạ tầng CNTT và hệ thống giám sát hiện hữu

Thời gian qua, dưới sự nỗ lực của Ban Chỉ đạo chuyển đổi số và Sở Thông tin và Truyền thông, hệ thống bảo vệ và giám sát an toàn thông tin mạng của tỉnh Đắk Lắk đã được định hình và từng bước phát huy hiệu quả. Về mặt hạ tầng cốt lõi, Trung tâm Tích hợp dữ liệu của tỉnh đã được đầu tư nâng cấp với quy mô 15 máy chủ vật lý, 212 máy chủ ảo hóa (VM), kết nối thông qua 06 thiết bị lưu trữ mạng (SAN). Hệ thống này duy trì đường truyền mạng số liệu chuyên dùng cấp 2 kết nối thông suốt đến 19 sở, ban, ngành, 15 UBND cấp huyện và 184 xã, phường, thị trấn trên toàn địa bàn. Tỉnh cũng đã hoàn thành công tác bảo đảm an toàn thông tin 4 lớp và thiết lập kết nối chia sẻ dữ liệu với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

Hiệu quả của hệ thống giám sát tập trung (SOC) hiện hữu được minh chứng bằng các số liệu cụ thể: trong một chu kỳ đánh giá, hệ thống đã phát hiện và ghi nhận 9.427 cảnh báo tấn công nhắm vào máy chủ và máy tính người dùng. Đồng thời, hệ thống bảo vệ vòng ngoài đã ghi nhận và ngăn chặn thành công hơn 3,7 triệu lượt tấn công rà quét khai thác lỗ hổng ứng dụng Web, cùng với 19.023 cuộc tấn công từ chối dịch vụ phân tán (DDoS) ở tầng ứng dụng (Layer 7). Những con số này phản ánh năng lực kỹ thuật rất đáng ghi nhận của đội ngũ quản trị trong việc bảo vệ tính toàn vẹn của các Cổng thông tin điện tử và hệ thống dịch vụ công.

Tuy nhiên, dưới góc độ phân tích kiến trúc hệ thống chuyên sâu và quản trị rủi ro tổng thể, Viện Kinh tế, Pháp luật và Quản lý chỉ ra rằng năng lực phòng thủ của tỉnh đang tập trung quá nhiều vào "chu vi mạng" (Perimeter Defense) mà thiếu vắng chiều sâu cần thiết để chống lại các mối đe dọa phức tạp từ bên trong.

2. Định vị các lỗ hổng kiến trúc và rủi ro phổ biến đang hiện hữu

Sự thiếu đồng bộ trong kiến trúc tổng thể dẫn đến 03 nhóm lỗ hổng cốt lõi mang tính hệ thống, tiềm ẩn nguy cơ phá vỡ toàn bộ nỗ lực chuyển đổi số của tỉnh:

+ **Thứ nhất, tính thụ động của Hệ thống Giám sát SOC và sự thiếu vắng cơ chế kiểm thử liên tục:** Mặc dù SOC hiện tại xử lý hàng ngàn cảnh báo, quy trình này mang tính chất "phản ứng sau sự kiện" (Reactive). Các hệ thống bảo vệ như Tường lửa (Firewall), Hệ thống ngăn chặn xâm nhập (IPS), hay Cổng lọc Web (WAF) thường được cấu hình tĩnh bằng các bộ quy tắc (rule-based) thủ công. Việc thiếu vắng một Hệ thống Giả lập Tấn công và Đánh giá Tự động (BAS) khiến đội ngũ quản trị không thể đo lường được liệu các thiết bị bảo mật đắt tiền này có thực sự chống đỡ được các kỹ thuật tấn công mới nhất hay không. Lỗ hổng cấu hình (misconfigurations) thường không bị phát hiện cho đến khi sự cố thực

sự xảy ra. Thêm vào đó, năng lực giám sát tại lớp thiết bị đầu cuối (Endpoint) ở tuyến huyện, xã còn mỏng, thiếu vắng cơ chế Phát hiện và Phản hồi tại thiết bị đầu cuối (EDR) được quản trị tập trung, khiến mã độc có thể lây lan âm thầm trong mạng lưới mạng diện rộng (MetroNet) trước khi bị phát hiện.

+ **Thứ hai, lỗ hổng nghiêm trọng trong chiến lược Quản trị Dữ liệu và thiếu hụt nền tảng chống thất thoát dữ liệu (DLP):** Đắk Lắk đã đạt những thành tựu lớn trong việc số hóa, đặc biệt là triển khai Đề án 06 với việc xây dựng 100% CSDL Hộ tịch điện tử, 100% CSDL quốc gia về cán bộ công chức, và hoàn thiện cơ bản CSDL đất đai. Tuy nhiên, nghịch lý nằm ở chỗ: dữ liệu càng hội tụ, rủi ro lộ lọt càng tập trung. Hiện tại, kiến trúc an ninh của tỉnh dường như thiếu vắng hoàn toàn một Nền tảng Chống thất thoát dữ liệu (DLP) có năng lực kiểm soát dữ liệu trên cả 3 trạng thái: dữ liệu đang lưu trữ (Data at rest), dữ liệu đang luân chuyển trên mạng (Data in motion), và dữ liệu đang được sử dụng tại máy trạm (Data in use). Thiếu vắng DLP và hệ thống Quản trị Tư thế Bảo mật Dữ liệu (DSPM) đồng nghĩa với việc quản trị viên không thể biết chính xác dữ liệu nhạy cảm (PII) đang nằm ở đâu, ai đang truy cập, và có bị sao chép trái phép ra các nền tảng đám mây công cộng hay thiết bị lưu trữ cá nhân hay không. Đây là điểm chí mạng khi Luật Bảo vệ dữ liệu cá nhân 2025 đi vào thực thi.

+ **Thứ ba, sự phân mảnh trong kiểm soát danh tính, đặc quyền và tính toàn vẹn hệ thống:** Sự phân mảnh thể hiện ở việc quản lý tài khoản có đặc quyền quản trị các hệ thống lõi. Thiếu vắng giải pháp Quản lý truy cập đặc quyền (PAM) và Giám sát hoạt động Cơ sở dữ liệu (DAM) tạo ra kẽ hở cho các cuộc tấn công nội bộ hoặc đánh cắp thông tin tài khoản. Khi một kỹ sư bảo trì đăng nhập vào máy chủ cơ sở dữ liệu y tế hoặc dân cư, nếu không có hệ thống PAM để ghi lại toàn bộ phiên làm việc và giới hạn câu lệnh, rủi ro can thiệp trái phép là không thể kiểm soát. Đồng thời, tỉnh cũng thiếu các giải pháp Giám sát tính toàn vẹn hệ thống (FIM), khiến cho việc phục hồi cấu hình hệ thống hoặc nội dung website sau khi bị tấn công thay đổi giao diện (Defacement) phải thực hiện thủ công, mất nhiều thời gian và ảnh hưởng đến tính sẵn sàng của dịch vụ công.

3. Đánh giá mức độ tác động của rủi ro đối với các hệ sinh thái

Sự hội tụ của các lỗ hổng trên tạo ra những rủi ro bất đối xứng đối với từng phân hệ trên địa bàn tỉnh:

+ **Đối với Khối Cơ quan hành chính Nhà nước (từ UBND tỉnh đến cấp xã):** Nguy cơ lớn nhất là các cuộc tấn công Ransomware mã hóa dữ liệu cục bộ hoặc hệ thống. Nếu một cán bộ xã nhấp vào một email lừa đảo (Phishing), mã độc có thể lan truyền qua mạng diện rộng về Datacenter tỉnh. Việc gián đoạn dịch vụ công trực tuyến không chỉ gây thiệt hại về kinh tế mà còn ảnh hưởng trực tiếp đến uy tín của chính quyền. Hơn nữa, nếu xảy ra lộ lọt dữ liệu từ Đề án 06, chính quyền sẽ phải đối mặt với các khủng hoảng về mặt pháp

lý và truyền thông.

+ Đối với Lực lượng thực thi pháp luật (tiêu biểu là Phòng PA05 - Công an tỉnh): Tội phạm công nghệ cao ngày càng sử dụng các phương thức ẩn danh tinh vi trên Dark Web hoặc thông qua các nền tảng tiền ảo. Sự thiếu hụt các hệ thống điều tra số chuyên sâu (Cyber Investigation) và hệ thống tình báo nguồn mở (OSINT) có khả năng phân tích biểu đồ quan hệ (Social Links) sẽ cản trở đáng kể năng lực trinh sát, truy vết, và thu thập chứng cứ điện tử hợp pháp của lực lượng chuyên trách.

+ Đối với Khối doanh nghiệp và Khu công nghiệp địa phương: Các doanh nghiệp tại KCN Hòa Phú khi ứng dụng IoT và 5G sẽ đối mặt với các cuộc tấn công vào hệ thống điều khiển công nghiệp (ICS/SCADA). Sự cố an ninh mạng tại đây có thể dẫn đến việc dây chuyền sản xuất bị đình trệ vật lý, gây thiệt hại hàng tỷ đồng mỗi giờ. Đồng thời, các doanh nghiệp xuất khẩu nếu không có cơ chế quản trị quyền đồng ý (Consent Management System) và Đánh giá tác động dữ liệu (PIA) sẽ dễ dàng vi phạm Nghị định 356/2025/NĐ-CP, đối diện với mức phạt kinh tế khổng lồ.

+ Đối với Hệ sinh thái Y tế và Giáo dục (ví dụ: Bệnh viện Sản Nhi tỉnh Đắk Lắk): Đây là những đơn vị lưu trữ lượng lớn dữ liệu cá nhân nhạy cảm nhất (hồ sơ bệnh án, thông tin di truyền, dữ liệu trẻ em). Mức độ bảo vệ tại các hệ thống này hiện chưa tương xứng với giá trị của dữ liệu. Bất kỳ sự cố lộ lọt hoặc mã hóa tống tiền nào cũng có thể đe dọa trực tiếp đến tính mạng và quyền riêng tư của bệnh nhân.

III. MỤC TIÊU CHIẾN LƯỢC CỦA ĐỀ ÁN

Đề án được xây dựng dựa trên triết lý quản trị rủi ro toàn diện: chuyển dịch từ mô hình "phòng thủ thụ động dựa trên chu vi" sang mô hình "chủ động thích ứng, lấy dữ liệu làm trung tâm (Data-centric) và xác thực không tin cậy (Zero-Trust)". Mục tiêu tối thượng là kiến tạo một hệ sinh thái an ninh số hội tụ, bảo đảm hạ tầng CNTT của tỉnh Đắk Lắk phát triển bền vững, trở thành bệ phóng an toàn vững chắc cho Chính phủ số, Kinh tế số và Xã hội số, đồng thời tuân thủ tuyệt đối các quy định của pháp luật về an toàn thông tin và bảo vệ dữ liệu.

1. Phân kỳ mục tiêu và hệ thống Chỉ số đánh giá hiệu năng định lượng

Quá trình chuyển dịch kiến trúc an ninh mạng được thiết kế theo lộ trình 05 năm, chia thành 03 giai đoạn với các mục tiêu và thước đo KPI nghiêm ngặt:

Phân kỳ Giai đoạn	Tiêu điểm Chiến lược	Chỉ số đánh giá hiệu năng (KPIs) định lượng bắt buộc đạt được
Ngắn hạn (Năm 1: 2026)	Thiết lập nền tảng phòng thủ vững chắc và tuân thủ pháp lý toàn diện. Trọng tâm là đáp ứng ngay lập tức các yêu cầu của Luật Bảo vệ DLCN 2025 và bảo đảm an toàn cho các hệ thống phục vụ Đề án 06.	• 100% hệ thống thông tin từ cấp độ 3 trở lên được lập, thẩm định và phê duyệt hồ sơ đề xuất cấp độ ATTT theo quy định. • 100% máy chủ tại Datacenter và hệ thống máy trạm của khối cơ quan hành chính cấp tỉnh, huyện được cài đặt và quản trị tập trung giải pháp bảo vệ thiết bị đầu cuối tiên tiến (Endpoint Security/EDR). • Hoàn thành quy trình Đánh giá tác động xử lý dữ liệu (PIA) theo chuẩn Nghị định 356/2025/NĐ-CP cho toàn bộ các hệ thống có kết nối với CSDL Quốc gia về dân cư. • Giảm thiểu ít nhất 50% tỷ lệ lây nhiễm sự cố mã độc tại các cơ quan hành chính tuyến cơ sở so với trung bình giai đoạn 2022-2024.
Trung hạn (Năm 3: 2028)	Mở rộng năng lực giám sát chủ động và kiểm soát dữ liệu chiều sâu. Trọng tâm là nâng cấp Trung tâm điều hành an ninh mạng (SOC) và kiểm soát hoàn toàn sự di chuyển	• Nâng cấp SOC tỉnh đạt chuẩn hội tụ tích hợp: Kết nối thành công luồng log sự kiện từ lớp mạng, ứng dụng, dữ liệu (DAM) và quản trị truy cập đặc quyền (PAM) về một màn hình điều khiển trung tâm. • 100% Cổng thông tin điện tử của tỉnh và các sở ngành trọng yếu được trang

Phân kỳ Giai đoạn	Tiêu điểm Chiến lược	Chỉ số đánh giá hiệu năng (KPIs) định lượng bắt buộc đạt được
	của dữ liệu.	bị cơ chế tự động phục hồi tính toàn vẹn hệ thống (Self-healing FIM). • Triển khai nền tảng Chống thất thoát dữ liệu (DLP) bao phủ >80% cơ quan, tổ chức lưu trữ dữ liệu cá nhân nhạy cảm. • Thiết lập chuẩn kiến trúc bảo mật phân vùng mạng (Zero-Trust) cho 100% hệ thống mạng 5G và IoT tại Khu công nghiệp Hòa Phú và các cụm công nghiệp.
Dài hạn (Năm 5: 2030)	Tối ưu hóa quy trình, tự động hóa bằng AI và định hình năng lực phục hồi linh hoạt (Cyber Resilience). Trọng tâm là năng lực đối kháng chủ động và tự động hóa ứng cứu sự cố.	• Đạt mức tự động hóa 80% trong các quy trình phân tích và phản ứng sự cố thông qua hệ thống điều phối an ninh (SOAR). • 100% hệ thống lõi của tỉnh được kiểm thử bảo mật và giả lập tấn công liên tục (Continuous Security Validation - BAS). • Đưa Đắk Lắk lọt vào nhóm Top 15 toàn quốc về Chỉ số An toàn thông tin mạng trong bộ tiêu chí DTI. • Hoàn thiện trang bị hệ sinh thái điều tra số chuyên sâu (Cyber Investigation) cho lực lượng PA05 để chủ động trấn áp tội phạm mạng.

IV. NỘI DUNG ĐỀ ÁN: KIẾN TRÚC 5 TRỤ CỘT CHIẾN LƯỢC

Để chuyển hóa tầm nhìn và mục tiêu thành hiện thực, Đề án cấu trúc toàn bộ các hạng mục đầu tư và giải pháp thành 5 trụ cột chiến lược. Các giải pháp công nghệ được chuẩn hóa dưới ngôn ngữ quản trị kiến trúc hệ thống, đảm bảo tính trung lập, không phụ thuộc vào bất kỳ nhà cung cấp (vendor) đơn lẻ nào, đồng thời có khả năng tương thích và mở rộng linh hoạt theo sự phát triển của công nghệ số.

Trụ cột 1: Xây dựng nền tảng Hạ tầng An ninh số linh hoạt và bền bỉ:

- Mục tiêu cốt lõi: Thiết lập một phòng tuyến vững chắc trải dài từ lõi Trung tâm Dữ liệu (Datacenter) của tỉnh, lan tỏa qua mạng diện rộng MetroNet, xuống tận thiết bị đầu cuối tại cấp xã và mở rộng đến các hệ thống mạng không dây 5G tại các khu công nghiệp. Triết lý thiết kế dựa trên sự phân rã chu vi mạng truyền thống, bảo đảm lưu lượng dữ liệu được định tuyến an toàn và chống chịu được các tác động rủi ro vật lý.

- Mô hình kiến trúc logic: Triển khai mô hình Zero-Trust Network Access (ZTNA) kết hợp với Mạng diện rộng định nghĩa bằng phần mềm an mật (Secure SD-WAN). Trong mô hình này, việc xác định quyền truy cập không còn dựa trên vị trí mạng mà dựa trên danh tính người dùng, tình trạng bảo mật của thiết bị (Device Posture) và ngữ cảnh truy cập tại thời điểm thực.

Thành phần công nghệ cốt lõi:

Hệ thống Tường lửa thế hệ mới (Next-Generation Firewall - NGFW) tích hợp SD-WAN: Đây là bộ脑 điều hướng và bảo vệ lưu lượng mạng, sở hữu năng lực bóc tách lưu lượng mã hóa SSL, phân tích hành vi người dùng, và tích hợp Hệ thống phòng ngừa xâm nhập sâu đa lớp (IPS).

Giải pháp Bảo mật thiết bị đầu cuối quản trị tập trung (Unified Endpoint Security/EDR): Kiến trúc triển khai dựa trên mô hình Trung tâm dữ liệu chính và Trung tâm dự phòng thảm họa. Hệ thống EDR dùng thuật toán máy học để theo dõi hành vi, phát hiện tức thì Ransomware và chủ động ngắt kết nối thiết bị nhiễm bệnh.

Tình huống ứng dụng thực tế): Khắc phục rủi ro đứt gãy hạ tầng tại khối chính quyền tuyến xã: *Khi hạ tầng cáp quang truyền thống bị đứt do lũ cuốn, hệ thống SD-WAN tại UBND xã sẽ ngay lập tức tự động chuyển đổi định tuyến (Failover) toàn bộ lưu lượng dữ liệu nghiệp vụ sang đường truyền dự phòng 4G/5G, đảm bảo cán bộ xã vẫn truy cập liên thông phần mềm một cửa điện tử an toàn qua các gói tin đóng gói VPN.*

Trụ cột 2: Nâng cấp Trung tâm Giám sát và Tự động hóa Phản ứng sự cố:

- **Mục tiêu cốt lõi:** Chuyển dịch hoàn toàn từ mô hình SOC truyền thống sang Trung tâm Điều hành An ninh mạng thông minh có khả năng tự phát hiện các mối đe dọa tiên tiến, tự động hóa quy trình ứng cứu sự cố, và kiểm định liên tục sức mạnh phòng thủ.

- **Mô hình kiến trúc logic:** Kiến trúc SOC 2.0 được cấu thành từ 04 lớp chức năng chuyên biệt hoạt động tuần hoàn: Lớp Thu thập dữ liệu đa nguồn → Lớp Phân tích tương quan bằng Dữ liệu lớn → Lớp Tự động hóa và Điều phối phản ứng → Lớp Kiểm chứng và Giả lập Tấn công liên tục.

Thành phần công nghệ cốt lõi:

Nền tảng Giả lập Tấn công và Đánh giá Bảo mật Tự động (Breach and Attack Simulation - BAS): Triển khai các "đại lý AI" chuyên biệt liên tục giả lập hành vi tấn công để nhận diện chính xác điểm yếu trên hệ thống bảo mật.

Giải pháp Giám sát và Tự động Phục hồi Toàn vẹn Hệ thống (File Integrity Monitoring - FIM): Giám sát chiều sâu liên tục đối chiếu mã băm thực tế của các tệp tin hệ thống với một bản chụp chuẩn an toàn.

Nền tảng Kiểm thử bảo mật ứng dụng động (Dynamic Application Security Testing - DAST): Rà quét tự động các ứng dụng web để phát hiện các lỗ hổng nghiêm trọng.

Tình huống ứng dụng thực tế Bảo vệ tính toàn vẹn của Cổng thông tin điện tử tỉnh: *Nếu tin tặc sửa đổi trái phép giao diện cổng thông tin, hệ thống FIM lập tức phát hiện sự sai lệch, chặn đứng hành vi và kích hoạt cơ chế tự phục hồi về trạng thái an toàn nguyên gốc trong tích tắc.*

Trụ cột 3: Quản trị Vòng đời và Bảo vệ Dữ liệu Lõi

- **Mục tiêu cốt lõi:** Quản trị vòng đời dữ liệu minh bạch, kiểm soát chặt chẽ luồng di chuyển của dữ liệu nhạy cảm nhằm đáp ứng Luật Bảo vệ dữ liệu cá nhân 2025 và bảo vệ kho dữ liệu khổng lồ từ Đề án 06.

- **Mô hình kiến trúc logic:** Kiến trúc Bảo vệ dữ liệu hội tụ quản trị dữ liệu ở cả 3 trạng thái (Data at Rest, Data in Motion, Data in Use), sử dụng AI để dán nhãn phân loại nội dung.

Thành phần công nghệ cốt lõi:

Nền tảng Chống thất thoát dữ liệu chủ động (DLP) và Quản trị Tư thế Dữ liệu (DSPM): Dò quét, định danh dữ liệu nhạy cảm bằng OCR và kiểm soát hành vi sao chép, gửi qua email hoặc in ấn trái phép.

Hệ thống Giám sát hoạt động Cơ sở dữ liệu (DAM): Lập danh mục các trường dữ

liệu nhạy cảm bên trong CSDL, giám sát thời gian thực các câu lệnh truy vấn bất thường.

Trụ cột 4: Quản trị Danh tính, Đặc quyền và Khung Tuân thủ Pháp lý

- Mục tiêu cốt lõi: Thể chế hóa các quy trình quản trị rủi ro vào nền tảng công nghệ, bảo đảm tính giải trình pháp lý ở mức độ cao nhất và kiểm soát triệt để rủi ro từ nội bộ.

- Thành phần công nghệ cốt lõi:

Hệ thống Quản lý Truy cập Đặc quyền (PAM): Đóng vai trò như hầm chứa mật khẩu, hỗ trợ Ghi hình Phiên làm việc Đặc quyền (Privileged Session Recording).

Hệ sinh thái Giải pháp Tuân thủ Nghị định 356/2025/NĐ-CP: Bao gồm Phần mềm Đánh giá tác động về bảo vệ dữ liệu cá nhân (PIA), Hệ thống Quản trị Quyền đồng ý (CMS) và Hệ thống Quản lý Quyền chủ thể dữ liệu (DSR).

Trụ cột 5: Dịch vụ Đặc thù và Đào tạo Năng lực Cốt lõi

- Mục tiêu cốt lõi: Khắc phục triệt để mắt xích yếu nhất (Con người), trang bị công cụ tình báo mạng cho lực lượng thực thi pháp luật.

- Thành phần công nghệ cốt lõi:

Nền tảng Diễn tập Thực chiến (Cyber Range): Phòng thí nghiệm giả lập kiến trúc mạng để Đội Xanh diễn tập chống lại các kịch bản tấn công thực tế.

Hệ sinh thái Công cụ Điều tra số và Trinh sát mạng (OSINT / Cyber Investigation): Công cụ tình báo nguồn mở liên kết dữ liệu phân tán để lập biểu đồ quan hệ phục vụ lực lượng Công an tỉnh.

Dịch vụ Đào tạo Nhận thức và Diễn tập Phishing.

V. KIẾN TRÚC TỔNG THỂ HỆ THỐNG

Để đảm bảo tính logic, khả năng tích hợp và khả năng mở rộng, Đề án kiến trúc an ninh thông tin tỉnh Đắk Lắk được phân rã thành 04 tầng (Layers) kết nối bởi các luồng dữ liệu bảo mật và được kiểm soát bằng các điểm chốt chặn (Control Points) nghiêm ngặt.

Phân lớp Kiến trúc	Nền tảng / Thành phần tham gia	Bản chất Dữ liệu & Cơ chế Bảo vệ cốt lõi
Edge / Network	KCN (IoT/5G), UBND Xã/Huyện, SD-WAN, NGFW	Lưu lượng vật lý & IP. Áp dụng Zero-Trust Network Access, IPS sâu và VPN động tự phục hồi.
SOC / Identity	Nền tảng SOC, BAS, SOAR, EDR, PAM	Event Logs & Mật khẩu đặc quyền. AI phân tích tương quan, liên tục giả lập tấn công (BAS) và ghi hình phiên làm việc (PAM).
Application	Cổng Dịch vụ công, API, Web, FIM, DAST	Mã nguồn & HTTP Traffic. Quét lỗ hổng liên tục, tự động chống thay đổi giao diện/cấu hình (Self-healing).
Data / Compliance	Đề án 06, CSDL Chuyên ngành, DLP, DAM, PIA	Dữ liệu nhạy cảm & Dữ liệu dân cư. Phân loại nội dung bằng OCR, chặn sao chép trái phép, kiểm soát SQL và xuất báo cáo PIA tự động.

VI. LỘ TRÌNH TRIỂN KHAI THỰC THI

Đề án áp dụng mô hình triển khai cuốn chiếu với phương châm hành động: "Thiết lập nền tảng vững chắc - Triển khai mở rộng thần tốc - Tối ưu hóa thông minh".

- Giai đoạn 1: Foundation (Năm 2026 - 2027) - Tổ chức phân loại kho dữ liệu, triển khai hệ thống PIA/CMS. Trang bị đồng bộ EDR để chống Ransomware. Gia cố Tường lửa NGFW và SD-WAN bảo mật cho khối phường/xã.

- Giai đoạn 2: Expansion (Năm 2028 - 2029) - Triển khai toàn diện nền tảng DLP, PAM, DAM. Đồng bộ chuẩn bảo mật Zero-Trust cho mạng 5G và IoT tại các KCN. Cung cấp công cụ OSINT cho lực lượng Công an tỉnh.

- Giai đoạn 3: Optimization (Năm 2030) - Tối ưu hóa hệ thống thông qua Nền tảng Giả lập tấn công (BAS) chạy tự động 24/7, tích hợp SOAR để giảm thời gian phản ứng sự cố xuống dưới 5 phút, và thiết lập cơ chế FIM tự phục hồi.

VII. HIỆU QUẢ KINH TẾ – XÃ HỘI VÀ ĐẢM BẢO QUỐC PHÒNG AN NINH

Việc thực thi Đề án sẽ tạo ra động lực phát triển bền vững, đóng góp trực tiếp vào mục tiêu đưa tỉnh Đắk Lắk trở thành trung tâm vùng Tây Nguyên:

- Nắm quyền chủ động pháp lý và quản trị rủi ro toàn diện: Tuân thủ khắt khe Luật Bảo vệ Dữ liệu cá nhân (số 91/2025/QH15) và ngăn ngừa các án phạt lớn từ thất thoát dữ liệu.

- Bảo vệ niềm tin công dân và tài nguyên dữ liệu: Kho dữ liệu khổng lồ hình thành từ Đề án 06 được mã hóa, định vị và bảo vệ khép kín trong không gian ảo.

- Tối ưu hóa hiệu năng hành chính: Hệ thống có năng lực phục hồi linh hoạt, đảm bảo hoạt động xuyên suốt, kể cả khi chịu ảnh hưởng thiên tai lũ lụt hay tấn công mạng.

- Hỗ trợ phát triển kinh tế số: Xây dựng "bệ phóng" hạ tầng số thu hút vốn FDI, cung cấp chuẩn mực an toàn cho KCN và chuỗi cung ứng toàn cầu.

- Bảo đảm An ninh Quốc gia và Trật tự Xã hội: Nâng cao năng lực tác chiến đối kháng cho Công an tỉnh, bóc gỡ tội phạm có tổ chức và dẹp bỏ các thế lực chống phá.

VIII. CƠ CHẾ TRIỂN KHAI VÀ MÔ HÌNH PHỐI HỢP LIÊN NGÀNH

Đề án áp dụng Mô hình quản trị đa bên:

- Ủy ban Nhân dân tỉnh Đắk Lắk: Chỉ đạo xuyên suốt, kiến tạo chính sách và phân bổ ngân sách dài hạn.

- Sở Thông tin và Truyền thông: Cơ quan thường trực quản lý, đóng vai trò "Tổng công trình sư" vận hành SOC hội tụ và quản trị hạ tầng.

- Công an tỉnh Đắk Lắk: Chịu trách nhiệm trực tiếp trong công tác trinh sát nguồn mở, đấu tranh bóc gỡ các hành vi tội phạm mạng.

- Cơ chế Xã hội hóa và Dịch vụ Thuê ngoài: Áp dụng cơ chế dịch vụ quản trị an ninh mạng thuê ngoài nhằm tận dụng triệt để nền tảng chuyên gia cao cấp và tối ưu chi phí đầu tư.

IX. KIẾN NGHỊ VÀ ĐỀ XUẤT TỪ VIỆN KINH TẾ, PHÁP LUẬT VÀ QUẢN LÝ

Căn cứ trên kết quả tổng hợp hiện trạng, Viện Kinh tế, Pháp luật và Quản lý trân trọng đệ trình các kiến nghị chiến lược sau đây:

1. Đối với Ủy ban nhân dân tỉnh Đắk Lắk: Kính đề nghị xem xét, phê duyệt định hướng Đề án làm văn kiện pháp lý nòng cốt. Khẩn trương ban hành Quy chế Quản trị Dữ liệu nội bộ cấp tỉnh để tuân thủ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15. Ưu tiên bố trí ngân sách dự phòng linh hoạt phục vụ ứng cứu sự cố.

2. Đối với các Sở, Ban, Ngành và UBND cấp Phường/Xã: Khẩn trương rà soát và thực hiện dứt điểm việc phê duyệt hồ sơ đề xuất cấp độ ATTT (đặc biệt các hệ thống cấp độ 3 trở lên). Các đơn vị quản lý kho dữ liệu chuyên ngành cần lập tức phối hợp chuẩn bị hồ sơ Đánh giá tác động xử lý dữ liệu cá nhân (PIA).

3. Đối với các đối tác công nghệ và Tập đoàn triển khai dịch vụ: Phải cam kết cung cấp giải pháp dựa trên tiêu chuẩn mở, tích hợp API trơn tru để chống tình trạng khóa chặt công nghệ (Vendor lock-in). Các giải pháp lõi bắt buộc phải có chứng chỉ kiểm định an toàn quốc tế (ISO 27001, Common Criteria, FIPS).

Viện Kinh tế, Pháp luật và Quản lý tin tưởng sâu sắc rằng, dưới sự chỉ đạo quyết liệt của lãnh đạo tỉnh, Đề án này sẽ kiến tạo "tấm khiên" số đa lớp vững chắc, giúp Đắk Lắk bứt phá trở thành một điểm sáng của khu vực Tây Nguyên về phát triển kinh tế số an toàn, thịnh vượng và bền vững.

VIỆN KINH TẾ, PHÁP LUẬT VÀ QUẢN LÝ

TS. Phan Ngọc Dũng

Viện trưởng kiêm Chủ tịch HĐKH