

Số: 5390 /KH-UBND

Lai Châu, ngày 30 tháng 6 năm 2026

KẾ HOẠCH

Thực hiện Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” trên địa bàn tỉnh Lai Châu

Thực hiện Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” (sau đây gọi tắt là Đề án), Công văn số 2522/BCA-A05 ngày 27/5/2026 của Bộ Công an về thông báo việc ban hành Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ. Ủy ban nhân dân (UBND) tỉnh Lai Châu ban hành Kế hoạch thực hiện Đề án như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

Cụ thể hóa và triển khai hiệu quả các quan điểm, mục tiêu, nhiệm vụ và giải pháp của Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ phù hợp với điều kiện thực tiễn trên địa bàn tỉnh Lai Châu, gắn với thực hiện các chỉ tiêu, nhiệm vụ về bảo đảm an ninh mạng.

2. Yêu cầu

- Đảm bảo việc triển khai thống nhất, đồng bộ, bám sát mục tiêu, nội dung của Đề án; phù hợp với chủ trương của Đảng, chính sách, pháp luật của Nhà nước và tình hình thực tiễn của tỉnh.

- Xác định rõ nội dung, trách nhiệm chủ trì, phối hợp của các cơ quan, đơn vị, địa phương; bảo đảm tiến độ, lấy kết quả làm thước đo.

II. MỤC TIÊU

1. Mục tiêu tổng quát

Nâng cao năng lực tổng thể, xây dựng lực lượng bảo vệ an ninh mạng của tỉnh tinh nhuệ, hiện đại; chủ động phòng ngừa, sẵn sàng ứng phó hiệu quả với các nguy cơ, thách thức trên không gian mạng; bảo vệ vững chắc an ninh quốc gia, trật tự, an toàn xã hội và quyền, lợi ích hợp pháp của tổ chức, cá nhân.

2. Mục tiêu đến năm 2030

- Triển khai hiệu quả công tác an ninh mạng, bảo mật thông tin, an ninh dữ liệu tại địa phương, góp phần thực hiện mục tiêu nâng cao năng lực bảo đảm an ninh mạng theo Quyết định số 515/QĐ-TTg.

- Phát triển nguồn nhân lực an ninh mạng của tỉnh; phấn đấu trên địa bàn tỉnh có chuyên gia an ninh mạng chuyên sâu, từng bước tiếp cận trình độ khu vực và quốc tế.

- Tổ chức triển khai các quy định, chương trình, nội dung đào tạo, tập huấn về kiến thức, kỹ năng an ninh mạng; quản lý, tổ chức thực hiện hoạt động đào tạo, bồi dưỡng và chứng nhận theo quy định.

- 100% lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5, trong cơ quan, tổ chức, doanh nghiệp Nhà nước có chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng do cơ quan có thẩm quyền cấp; được cập nhật kiến thức an ninh mạng ít nhất 01 lần/năm.

- 90% người sử dụng Internet có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an ninh mạng.

- Thiết lập cơ chế chia sẻ thông tin, cảnh báo, điều phối ứng phó sự cố giữa các lực lượng bảo vệ an ninh mạng và các doanh nghiệp an ninh mạng trên địa bàn để nâng cao năng lực phòng thủ tỉnh.

- 70% các sở, ban, ngành tỉnh và Ủy ban nhân dân các xã, phường và các hệ thống thông tin quan trọng quốc gia sử dụng sản phẩm công nghệ chiến lược “Make in Vietnam”; 100% các sản phẩm, dịch vụ an ninh mạng phải được kiểm định, đánh giá trước khi đưa vào sử dụng, áp dụng trước hết đối với hệ thống thông tin của các cơ quan trong hệ thống chính trị có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân.

- 100% các hệ thống thông tin sử dụng vốn ngân sách nhà nước được triển khai đầy đủ các phương án bảo đảm an ninh mạng theo cấp độ.

III. NỘI DUNG NHIỆM VỤ

1. Nhiệm vụ chung

1.1. Hoàn thiện thể chế, xây dựng và triển khai các cơ chế, chính sách đặc thù

- Rà soát, cập nhật, hoàn thiện các văn bản quy phạm pháp luật, văn bản hướng dẫn về bảo đảm an ninh mạng thuộc thẩm quyền của tỉnh; tổ chức triển khai thống nhất, đồng bộ các quy định của Trung ương.

- Tổ chức triển khai áp dụng tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng; thực hiện đánh giá, kiểm tra, giám sát việc tuân thủ đối với các hệ thống thông tin thuộc phạm vi quản lý, ưu tiên hệ thống thông tin quan trọng.

- Triển khai áp dụng mô hình quản lý rủi ro an ninh mạng tại các cơ quan, đơn vị; từng bước chuyển từ quản lý kỹ thuật sang quản trị rủi ro tổng thể.

- Thực hiện các cơ chế, chính sách thu hút, đào tạo, bồi dưỡng nguồn nhân lực an ninh mạng trên địa bàn tỉnh.

1.2. Tổ chức lực lượng an ninh mạng

- củng cố, kiện toàn Tiểu ban An ninh mạng tỉnh.

- Phân công, xây dựng mô hình tổ chức lực lượng thực hiện công tác bảo đảm an ninh mạng tại các cơ quan, đơn vị, địa phương và các tổ chức quản lý, vận hành hệ thống thông tin quan trọng về an ninh quốc gia trên địa bàn tỉnh theo hướng dẫn của Trung ương.

- Xây dựng, phát triển mạng lưới chuyên gia an ninh mạng trên địa bàn tỉnh; kết nối, tham gia vào mạng lưới chuyên gia, mạng lưới ứng cứu sự cố an ninh mạng quốc gia; hoàn thiện cơ chế trao đổi, chia sẻ thông tin và quy trình phối hợp xử lý sự cố giữa các cơ quan, đơn vị, địa phương và với Trung ương.

- Phát triển đội ngũ cán bộ, chuyên gia an ninh mạng của tỉnh có năng lực chuyên sâu, từng bước tiếp cận các công nghệ mới.

1.3. Đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao

- Triển khai áp dụng tiêu chuẩn chức danh, vị trí việc làm, khung kiến thức, kỹ năng an ninh mạng, các quy định về đào tạo, sát hạch, cấp chứng nhận theo hướng dẫn của Trung ương.

- Xây dựng, tổ chức triển khai các chương trình, tài liệu đào tạo, tập huấn về bảo vệ an ninh mạng; chuẩn hóa hoạt động đào tạo an ninh mạng phù hợp với từng nhóm đối tượng.

- Hằng năm, trên cơ sở khảo sát nhu cầu thực tiễn, tổ chức các khóa đào tạo, tập huấn (trực tiếp, trực tuyến hoặc kết hợp) cho cơ quan, tổ chức, đơn vị trong toàn hệ thống chính trị trên địa bàn tỉnh, bao gồm: (1) Bồi dưỡng kiến thức cho lãnh đạo, quản lý; (2) Trang bị kỹ năng cho người sử dụng; (3) Đào tạo chuyên sâu cho lực lượng chuyên trách, lực lượng bảo vệ an ninh mạng, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, 4, 5.

- Tổ chức các chương trình diễn tập an ninh mạng cấp tỉnh; tham gia các chương trình diễn tập an ninh mạng cấp bộ, ngành, khu vực theo phân công nhằm nâng cao năng lực ứng phó và phối hợp xử lý sự cố an ninh mạng.

- Phối hợp đưa kiến thức an ninh mạng vào chương trình giáo dục phổ thông (từ trung học cơ sở đến trung học phổ thông), giáo dục nghề nghiệp và đại học; tổ chức cuộc thi, diễn đàn, câu lạc bộ an ninh mạng học đường và duy trì hoạt động hằng năm.

- Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, “Bình dân học vụ số”, các khóa học trực tuyến đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng.

- Triển khai, phối hợp xây dựng và sử dụng các nền tảng quản lý đào tạo, đánh giá, chứng nhận kỹ năng; quản lý dữ liệu chứng chỉ và phát triển cơ sở dữ liệu chuyên gia an ninh mạng trên địa bàn tỉnh.

- Tăng cường liên kết giữa cơ quan nhà nước, cơ sở đào tạo, doanh nghiệp trong phát triển nguồn nhân lực an ninh mạng.

1.4. Giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng

- Triển khai áp dụng bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng đối với các cơ quan, đơn vị trên địa bàn tỉnh.

- Tham gia, kết nối hệ thống chia sẻ thông tin, cảnh báo an ninh mạng; thúc đẩy chia sẻ thông tin giữa cơ quan nhà nước và doanh nghiệp.

- Xây dựng, triển khai nền tảng giám sát, điều hành an ninh mạng cho phép báo cáo, thống kê, cập nhật dữ liệu an ninh mạng trên địa bàn tỉnh, đảm bảo dữ liệu “đúng, đủ, sạch, sống, dùng chung, thống nhất”.

1.5. Nghiên cứu, phát triển và ứng dụng công nghệ

- Khuyến khích, hỗ trợ doanh nghiệp nghiên cứu, phát triển, cung cấp sản phẩm, dịch vụ an ninh mạng; ưu tiên sử dụng sản phẩm “Make in Vietnam”.

- Tăng cường phối hợp với các cơ quan Trung ương, doanh nghiệp trong nghiên cứu, ứng dụng, chuyển giao công nghệ an ninh mạng.

1.6. Tăng cường hợp tác quốc tế

- Chủ động thiết lập, mở rộng hợp tác với các địa phương, tổ chức, doanh nghiệp nước ngoài trong chia sẻ kinh nghiệm, hỗ trợ kỹ thuật và đào tạo về an ninh mạng.

- Tham gia các diễn đàn, hội nghị, hoạt động hợp tác, chia sẻ kinh nghiệm về an ninh mạng theo phân công.

- Khuyến khích cán bộ, chuyên gia tham gia các hoạt động chuyên môn, hội thảo, cuộc thi trong và ngoài nước.

- Lồng ghép nội dung hợp tác an ninh mạng trong hoạt động đối ngoại của tỉnh; duy trì trao đổi, phối hợp với các đối tác quốc tế theo phân cấp.

2. Nhiệm vụ cụ thể: (có phụ lục kèm theo).

III. KINH PHÍ THỰC HIỆN

Được bố trí trong dự toán hằng năm theo phân cấp ngân sách nhà nước và các nguồn hợp pháp khác theo quy định của pháp luật.

IV. TỔ CHỨC THỰC HIỆN

1. Căn cứ nội dung Kế hoạch, các cơ quan, đơn vị, địa phương theo chức năng, nhiệm vụ được giao, tổ chức triển khai, cụ thể hóa bằng văn bản, hình thức cụ thể. Định kỳ hàng năm (trước ngày 10/12) báo cáo kết quả, tiến độ triển khai thực hiện về UBND tỉnh (qua Công an tỉnh).

2. Công an tỉnh chủ trì hướng dẫn, đôn đốc, kiểm tra việc thực hiện Kế hoạch này; kịp thời tổng hợp, báo cáo Ủy ban nhân dân tỉnh xử lý, giải quyết các vấn đề phát sinh trong quá trình triển khai thực hiện; thực hiện chế độ thông tin, báo cáo định kỳ, đột xuất theo quy định.

Kế hoạch này thay thế Công văn 2998/UBND-TH ngày 21/4/2026 của UBND tỉnh về triển khai thực hiện Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia”.

Trong quá trình thực hiện, nếu có khó khăn vướng mắc, các cơ quan, đơn vị, địa phương báo cáo về Ủy ban nhân dân tỉnh (qua Công an tỉnh tổng hợp), để xem xét, giải quyết hoặc báo cáo cấp có thẩm quyền chỉ đạo, giải quyết./.

Nơi nhận:

- Văn phòng Chính phủ;
- Bộ Công an;
- TT Tỉnh ủy;
- TT HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Ủy ban MTTQ Việt Nam tỉnh;
- Các sở, ban, ngành tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Ban Chỉ huy Bộ đội Biên phòng;
- UBND các xã, phường;
- VP UBND tỉnh: V, C;
- Lưu: VT, Th4.

} (b/c)

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

Hà Quang Trung