ỦY BAN NHÂN DÂN
TỈNH SƠN LA

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

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 Sơn La

(*Kèm theo Quyết định số* 1073 */QĐ-UBND ngày* 02 *tháng* 05 *năm 2026 của Chủ tịch Ủy ban nhân dân tỉnh*)

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Tổ chức triển khai đồng bộ, hiệu quả các nhiệm vụ, giải pháp của Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" ban hành kèm theo Quyết định số 515/QĐ-TTg ngày 30/3/2025 của Thủ tướng Chính phủ (sau đây gọi tắt là Đề án).

- Xác định cụ thể nội dung công việc, thời hạn, tiến độ hoàn thành, cơ chế phối hợp và trách nhiệm của các cơ quan, đơn vị, tổ chức có liên quan trong triển khai Đề án.

- Nâng cao năng lực bảo vệ an ninh mạng, góp phần bảo đảm an ninh, trật tự phục vụ phát triển kinh tế - xã hội trên địa bàn tỉnh.

2. Yêu cầu

- Bảo đảm sự chỉ đạo thống nhất của Ủy ban nhân dân tỉnh, Chủ tịch Ủy ban nhân dân tỉnh; sự phối hợp chặt chẽ, thường xuyên, hiệu quả giữa các sở, ban, ngành của tỉnh; các đơn vị sự nghiệp công lập trực thuộc Ủy ban nhân dân tỉnh; Ủy ban nhân dân các xã, phường và các cơ quan, tổ chức có liên quan trong việc triển khai Đề án.

- Người đứng đầu cơ quan, tổ chức, đơn vị, địa phương được giao nhiệm vụ chủ động triển khai thực hiện Kế hoạch này theo đúng tiến độ, bảo đảm tính thống nhất, chất lượng, thiết thực, hiệu quả.

- Thường xuyên kiểm tra, đôn đốc, hướng dẫn, kịp thời giải quyết những khó khăn, vướng mắc trong quá trình triển khai Đề án.

II. MỤC TIÊU

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

2. Mục tiêu đến năm 2030

- 100% lực lượng bảo vệ an ninh mạng của Ủy ban nhân dân tỉnh, 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.

- Kết nối, chia sẻ thông tin, cảnh báo, điều phối ứng phó sự cố giữa lực lượng bảo vệ an ninh mạng của Ủy ban nhân dân tỉnh và các doanh nghiệp an ninh mạng để nâng cao năng lực phòng thủ.

- 70% các sở, ngành, địa phương và các hệ thống thông tin quan trọng quốc gia trên địa bàn tỉnh 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 hạ tầng thông tin quan trọng quốc gia, 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. NHIỆM VỤ VÀ GIẢI PHÁP

1. Hoàn thiện thể chế, xây dựng và triển khai các cơ chế, chính sách đặc thù về an ninh mạng

a) Tham gia rà soát, cập nhật, hoàn thiện các văn bản quy phạm pháp luật và văn bản hướng dẫn công tác an ninh mạng bảo đảm đồng bộ, thống nhất, hiệu quả giữa các lực lượng, đáp ứng yêu cầu quản lý, bảo vệ không gian mạng.

b) Triển khai Công ước Liên Hợp quốc về chống tội phạm mạng.

c) Triển khai các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật đối với các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, áp dụng trước hết đối với hạ tầng thông tin quan trọng quốc gia, 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.

d) Triển khai khung quản lý rủi ro an ninh mạng quốc gia, chuyển đổi từ quản lý kỹ thuật thuần túy sang quản trị rủi ro toàn diện nhằm tăng tính chủ động của các cơ quan, tổ chức trong việc phân bổ nguồn lực, giảm thiểu tổn thất từ các cuộc tấn công.

đ) Tiếp tục nghiên cứu, hoàn thiện, tổ chức triển khai có hiệu quả các cơ chế và chính sách ưu đãi nhằm thu hút, trọng dụng, bồi dưỡng, nâng cao chất lượng nguồn nhân lực cho lực lượng bảo vệ an ninh mạng trên phạm vi toàn tỉnh.

2. Tổ chức lực lượng an ninh mạng

a) Tham mưu triển khai có hiệu quả hoạt động của Tiểu ban An ninh mạng tỉnh.

b) Tổ chức lực lượng bảo vệ an ninh mạng tại Ủy ban nhân dân tỉnh theo hướng dẫn của Bộ Công an.

c) Triển khai có hiệu quả hoạt động của đội Ứng cứu sự cố an toàn thông tin mạng tỉnh. Kết nối, chia sẻ dữ liệu với Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam.

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

a) Hằng năm, chọn cử cán bộ tham gia các khóa đào tạo, tập huấn chuyên sâu kiến thức, kỹ năng an ninh mạng.

b) Hằng năm, tổ chức ít nhất 01 cuộc diễn tập an ninh mạng cấp tỉnh nhằm nâng cao năng lực chỉ huy, điều hành, phối hợp liên ngành và khả năng ứng phó, khắc phục sự cố an ninh mạng trong tình huống thực tế.

c) 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.

d) 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.

đ) Tăng cường liên kết giữa Nhà nước - Nhà trường - Doanh nghiệp trong đào tạo, huấn luyện thực chiến. Xây dựng mạng lưới chuyên gia an ninh mạng trong tỉnh, sẵn sàng huy động nguồn lực xã hội tham gia ứng cứu sự cố, tình huống nguy hiểm về an ninh mạng.

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

a) Triển khai bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng đối với cơ quan, đơn vị, tổ chức, doanh nghiệp.

b) Tiếp tục duy trì hệ thống giám sát an ninh mạng và hệ thống phần mềm phòng, chống mã độc theo mô hình tập trung của tỉnh.

c) Xây dựng và đưa vào vận hành Trung tâm An ninh mạng tỉnh theo mô hình phù hợp với điều kiện thực tiễn của tỉnh và hướng dẫn của Bộ Công an, phục vụ giám sát, phát hiện sớm, cảnh báo, phối hợp xử lý các nguy cơ, sự cố an ninh mạng đối với các hệ thống thông tin của tỉnh; kết nối, chia sẻ thông tin với các hệ thống giám sát an ninh mạng của Trung ương theo quy định.

5. Đẩy mạnh hợp tác, liên kết vùng, quốc tế trên lĩnh vực an ninh mạng

a) Tăng cường liên kết, hợp tác với các tỉnh, thành phố trong và ngoài nước để chia sẻ kinh nghiệm, hợp tác trong bảo đảm an ninh mạng, bảo mật dữ liệu, đào tạo nhân lực, xây dựng hạ tầng....

b) Chủ động tổ chức, tham gia các diễn đàn, hội thảo, hội nghị, học tập kinh nghiệm về an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

c) Tạo điều kiện cho các chuyên gia, nhà khoa học trong và ngoài nước đến địa phương làm việc, hợp tác.

IV. KINH PHÍ THỰC HIỆN

1. Kinh phí thực hiện Kế hoạch do ngân sách nhà nước đảm bảo theo phân cấp quản lý ngân sách hiện hành, được bố trí trong dự toán chi thường xuyên ngân sách nhà nước hàng năm của các sở, ban, ngành, đơn vị dự toán cấp tỉnh, UBND các xã, phường; nguồn kinh phí được giao bổ sung trong năm và các nguồn vốn hợp pháp khác theo quy định.

2. Việc lập dự toán, quản lý, sử dụng, thanh toán, quyết toán kinh phí thực hiện theo Luật Ngân sách nhà nước và các văn bản hướng dẫn thi hành.

V. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

a) Giúp Ủy ban nhân dân tỉnh thống nhất triển khai các hoạt động nâng cao năng lực lực lượng bảo vệ an ninh mạng trên địa bàn tỉnh và hướng dẫn các cơ quan, đơn vị, địa phương triển khai thực hiện bảo đảm chất lượng, hiệu quả.

b) Rà soát, sửa đổi, bổ sung theo thẩm quyền hoặc kiến nghị cơ quan có thẩm quyền sửa đổi, bổ sung, hoàn thiện, chính sách pháp luật về an ninh mạng, tổ chức lực lượng an ninh mạng tại điểm 1, điểm 2 Mục III.

c) Chủ trì, phối hợp với Sở Giáo dục và Đào tạo, Sở Nội vụ và các sở, ngành có liên quan triển khai các nhiệm vụ phát triển nguồn nhân lực an ninh mạng tại điểm 3 Mục III.

d) Chủ trì tham mưu xây dựng triển khai các giải pháp giám sát an ninh mạng, chia sẻ thông tin giám sát với Trung tâm An ninh mạng quốc gia tại điểm 4 Mục III.

đ) Định kỳ sơ kết, tổng kết, đánh giá tình hình thực hiện Kế hoạch này; trường hợp cần thiết, báo cáo Chủ tịch Ủy ban nhân dân tỉnh xem xét chỉnh sửa, bổ sung các nội dung liên quan thuộc Kế hoạch này nhằm phù hợp với tình hình thực tiễn.

2. Sở Khoa học và Công nghệ: tham mưu triển khai các nhiệm vụ, dự án phù hợp với ngành, lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số để triển khai Kế hoạch này theo chỉ đạo, hướng dẫn của Bộ Khoa học và Công nghệ.

3. Sở Giáo dục và Đào tạo: tham mưu triển khai các chương trình đào tạo nguồn nhân lực về an ninh mạng theo chỉ đạo, hướng dẫn của Bộ Giáo dục và Đào tạo.

4. Sở Nội vụ: phối hợp với Công an tỉnh trong triển khai tiêu chuẩn chuyên môn, nghiệp vụ cho lực lượng bảo vệ an ninh mạng, đề xuất cơ chế thu hút nhân lực chất lượng cao làm việc trong lĩnh vực an ninh mạng, cơ chế giữ nhân lực an ninh mạng làm việc tại cơ quan nhà nước.

5. Sở Tài chính: cân đối nguồn ngân sách nhà nước hằng năm cho lĩnh

vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số theo quy định của pháp luật về ngân sách, về đầu tư công và pháp luật quản lý ngành, lĩnh vực. Bảm đảm nguồn lực triển khai Kế hoạch này.

6. Bộ Chỉ huy Quân sự tỉnh

a) Triển khai đồng bộ, hiệu quả các giải pháp bảo đảm an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý.

b) Rà soát, hoàn thiện mô hình tổ chức lực lượng chuyên trách bảo vệ an ninh mạng thuộc phạm vi quản lý theo chỉ đạo, hướng dẫn của Bộ Quốc phòng.

c) Tổ chức tập huấn và chứng nhận kiến thức, kỹ năng chuyên sâu về an ninh mạng cho các đối tượng thuộc phạm vi quản lý.

d) Phối hợp chặt chẽ với Công an tỉnh trong triển khai các nhiệm vụ, giải pháp, đặc biệt là phát triển nguồn nhân lực, tổ chức giám sát, diễn tập an ninh mạng.

7. Sở Ngoại vụ: phối hợp với Công an tỉnh trong đẩy mạnh hợp tác, liên kết vùng, quốc tế trên lĩnh vực an ninh mạng tại điểm 5 Mục III.

8. Các sở, ngành, địa phương

a) Ưu tiên bố trí nguồn lực *(nhân lực, kinh phí)* và điều kiện để triển khai hoạt động bảo đảm an ninh mạng trong hoạt động nội bộ của cơ quan, đơn vị, địa phương và lĩnh vực quản lý.

b) Hằng năm chọn cử lãnh đạo, cán bộ tham gia diễn tập an ninh mạng cấp tỉnh, ứng cứu sự cố mạng trong phạm vi của của cơ quan, đơn vị và lĩnh vực quản lý.

c) Hằng năm theo chức năng, nhiệm vụ tổ chức tập huấn, cập nhật phổ biến, quán triệt, tuyên truyền các nội dung về bảo đảm an ninh mạng nhằm nâng cao năng lực, kiến thức, kỹ năng cho cán bộ, công chức, viên chức thuộc quyền quản lý *(gồm quản lý, lãnh đạo; người dùng cuối; nhân sự kỹ thuật an ninh mạng)*.

d) Trang bị hệ thống, công cụ chuyên dụng cho lực lượng bảo vệ an ninh mạng, tối thiểu gồm: hệ thống, công cụ rà quét phát hiện lỗ hổng bảo mật; hệ thống, công cụ hỗ trợ điều tra số, ứng cứu, khắc phục sự cố an ninh mạng.

đ) Đẩy mạnh hoạt động bảo đảm an ninh mạng trong phạm vi quản lý; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an, Công an tỉnh và quy định của pháp luật; ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng "Make in Vietnam". Gắn kết công tác bảo đảm an ninh mạng với công tác triển khai chuyển đổi số, ứng dụng công nghệ thông tin, phát triển Chính quyền số, đô thị thông minh, kinh tế số và xã hội số.

Quá trình thực hiện Kế hoạch này nếu có khó khăn, vướng mắc, đề nghị các cơ quan, đơn vị, địa phương kịp thời phản ánh về Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)* để tổng hợp, hướng dẫn, giải quyết theo thẩm quyền hoặc trình cấp có thẩm quyền xem xét, quyết định./.