TỈNH ỦY LAI CHÂU *	ĐẢNG CỘNG SẢN VIỆT NAM
Số 20-CTr/TU	*Lai Châu, ngày 07 tháng 4 năm 2026*

CHƯƠNG TRÌNH HÀNH ĐỘNG
thực hiện Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị

Thực hiện Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị, Ban Thường vụ Tỉnh ủy ban hành Chương trình hành động thực hiện như sau:

I- TÌNH HÌNH

Thời gian qua, Đảng và Nhà nước ta có nhiều chủ trương, chính sách đẩy mạnh ứng dụng, phát triển khoa học, công nghệ, thúc đẩy đổi mới sáng tạo và chuyển đổi số quốc gia. Công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị của tỉnh được triển khai thực hiện nghiêm túc, đạt được nhiều kết quả quan trọng. Nhận thức của cấp ủy, tổ chức đảng, cơ quan, đơn vị và cán bộ, đảng viên về vai trò, tầm quan trọng của an ninh mạng được nâng lên rõ rệt. Hệ thống hạ tầng công nghệ thông tin từng bước được đầu tư, nâng cấp, bước đầu bảo đảm yêu cầu về an toàn, an ninh thông tin; các biện pháp đảm bảo an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị được các cơ quan, đơn vị, địa phương triển khai, thực hiện hiệu quả. Việc vận hành các cơ sở dữ liệu được chú trọng, bảo đảm tính chính xác, đồng bộ, an toàn. Công tác đào tạo, bồi dưỡng kỹ năng về an ninh mạng cho cán bộ, công chức, viên chức được tăng cường. Qua đó, góp phần bảo vệ vững chắc hệ thống thông tin, dữ liệu, phục vụ hiệu quả công tác lãnh đạo, chỉ đạo, điều hành trong tình hình mới.

Bên cạnh kết quả đạt được, quy mô, tiềm lực, trình độ khoa học, công nghệ và đổi mới sáng tạo của tỉnh chưa đáp ứng nhu cầu phát triển chung, còn khoảng cách xa so với các tỉnh khác trong khu vực; hạ tầng, cơ sở vật chất, các biện pháp đảm bảo an ninh, an toàn thông tin, bảo vệ dữ liệu triển khai chưa đồng bộ, hiệu quả chưa cao.

Nguyên nhân của những hạn chế nêu trên chủ yếu là do nguồn kinh phí đầu tư cho công tác đảm bảo an ninh mạng, an toàn thông tin, bảo mật dữ liệu còn hạn chế; thiếu nguồn nhân lực chất lượng cao, có trình độ chuyên sâu về an ninh mạng, an toàn thông tin, nhất là tại cấp cơ sở; mức độ tự chủ về công nghệ, sản phẩm an ninh mạng chưa cao, cơ bản phụ thuộc nhà thầu cung cấp dịch vụ.

II- MỤC TIÊU, TẦM NHÌN

1. Mục tiêu chung

Xây dựng không gian mạng an toàn, vững mạnh, có năng lực phòng vệ tốt và khả năng chống chịu cao, tạo điều kiện để phát triển khoa học, công nghệ, đổi mới, sáng tạo, chuyển đổi số, đồng thời góp phần bảo vệ vững chắc chủ quyền, an ninh, lợi ích của tỉnh và quốc gia trên không gian mạng.

2. Mục tiêu đến năm 2030

- Tạo chuyển biến mạnh mẽ về nhận thức và hành động, phát huy vai trò của các cấp ủy trong lãnh đạo, chỉ đạo các nhiệm vụ về bảo đảm an ninh mạng.

- Có cơ chế, chính sách khuyến khích đổi mới, sáng tạo và tạo điều kiện cho doanh nghiệp mới tham gia thị trường có sản phẩm, giải pháp an ninh mạng chất lượng có cơ hội phát triển; các quy định của pháp luật đủ sức răn đe với các hành vi vi phạm pháp luật trên không gian mạng.

- Hoàn thiện cơ sở dữ liệu dùng chung kết nối liên thông với hệ thống thông tin, cơ sở dữ liệu quốc gia. Phát triển trung tâm giám sát an ninh mạng và điều hành thông minh của tỉnh đủ để bảo vệ dữ liệu của cá nhân và tổ chức. Các hệ thống thông tin của cơ quan, đơn vị, địa phương được kiểm tra, rà soát, khắc phục các lỗ hổng, điểm yếu an ninh mạng.

- Nâng cao nhận thức của cán bộ, đảng viên và người dân về bảo mật thông tin, an ninh mạng và an toàn dữ liệu; đào tạo, bồi dưỡng đội ngũ cán bộ chuyên trách, có chất lượng, đủ năng lực bảo vệ hạ tầng số trên địa bàn tỉnh.

- Triển khai đầy đủ giải pháp bảo đảm an toàn hệ thống thông tin theo cấp độ ngay từ khâu thiết kế, đầu tư, vận hành; ưu tiên các hệ thống nền tảng, hệ thống phục vụ thủ tục hành chính và hệ thống dữ liệu lõi; thực hiện quản trị mạng dựa trên đánh giá rủi ro, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật.

- Thúc đẩy ứng dụng các công nghệ tiên tiến như trí tuệ nhân tạo (AI), phân tích dữ liệu lớn (Big Data), giám sát thông minh để sớm phát hiện và xử lý kịp thời các mối đe dọa an ninh mạng. Chuyển đổi sang mô hình phòng thủ chủ động, áp dụng các giải pháp mã hóa hiện đại phục vụ bảo vệ dữ liệu quan trọng, dữ liệu bí mật. Tăng cường sử dụng các sản phẩm, dịch vụ an ninh mạng "Make in Vietnam". Khuyến khích các đơn vị nghiên cứu, phát triển, tự chủ về công nghệ đối với một số sản phẩm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

3. Tầm nhìn đến năm 2045

Phát triển hạ tầng an ninh mạng và hạ tầng số đồng bộ, hiện đại. Các hoạt động của hệ thống chính trị được vận hành trên nền tảng số, bảo đảm minh bạch, hiệu quả và phục vụ người dân, doanh nghiệp nhanh chóng, thuận tiện;

xây dựng đội ngũ cán bộ chuyên trách an ninh mạng có trình độ, đáp ứng nhu cầu của tỉnh; làm chủ công nghệ với một số sản phẩm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

III- NHIỆM VỤ, GIẢI PHÁP

1. Tăng cường sự lãnh đạo của các cấp ủy đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn dân về an ninh mạng, bảo mật thông tin, an ninh dữ liệu

a) Các cấp ủy, tổ chức đảng, cán bộ, đảng viên nhận thức đầy đủ, sâu sắc quan điểm, chủ trương, chính sách của Đảng, Nhà nước về chuyển đổi số, phát triển khoa học, công nghệ, đổi mới sáng tạo, an ninh mạng; xác định rõ trách nhiệm, chủ động thực hiện, trong đó nhiệm vụ bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ trọng yếu, thường xuyên; huy động sức mạnh tổng hợp của toàn dân, xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng, phát huy vai trò chủ chốt của lực lượng Công an nhân dân, Quân đội nhân dân.

b) Nâng cao nhận thức, quyết tâm, phát triển khoa học, công nghệ và đổi mới sáng tạo, thực hiện chuyển đổi số trong cả hệ thống chính trị, người dân và doanh nghiệp trên địa bàn tỉnh. Quán triệt phương châm "Tự chủ, tự lực, tự cường" trong xây dựng tiềm lực an ninh mạng. Tập trung phát triển, khai thác, sử dụng hệ sinh thái sản phẩm, dịch vụ an ninh mạng Việt Nam, ưu tiên làm chủ công nghệ lõi, giải pháp bảo mật tiên tiến, ứng dụng mạnh mẽ trí tuệ nhân tạo, công nghệ mới vào lĩnh vực an ninh mạng. Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, giáo dục kiến thức, kỹ năng an ninh mạng; phát huy trách nhiệm xã hội của cơ quan báo chí, người có uy tín, người có ảnh hưởng trên không gian mạng trong việc định hướng dư luận, lan toả thông tin tích cực và đấu tranh với các thông tin xấu độc. Tập trung đào tạo, nâng cao năng lực, kỹ năng của lực lượng chuyên trách về an ninh mạng.

c) Bảo đảm an ninh mạng, an ninh dữ liệu là yếu tố nền tảng, yêu cầu bắt buộc ngay từ khâu quy hoạch, thiết kế, xây dựng, vận hành hệ thống thông tin. Hệ thống chưa bảo đảm an toàn, an ninh thì kiên quyết chưa đưa vào sử dụng; nhận diện và xử lý từ sớm, từ xa những nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an ninh dữ liệu để có biện pháp phòng vệ. Thường xuyên rà soát, kiểm tra, đánh giá an ninh mạng đối với các hệ thống công nghệ thông tin. Việc thu thập, quản lý, khai thác dữ liệu số phải được bảo vệ ở mức độ cao nhất; tuyệt đối không để lộ, lọt bí mật nhà nước, dữ liệu nhạy cảm, ngay cả trong quá trình thử nghiệm.

d) Người đứng đầu cấp ủy, chính quyền, cơ quan, đơn vị, địa phương chịu trách nhiệm trực tiếp, toàn diện về công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước tại cơ quan, đơn vị, địa phương mình. Cán bộ,

đảng viên, công chức, viên chức và người lao động phải gương mẫu thực hiện. Kết quả công tác này là một trong những tiêu chí quan trọng để đánh giá, xếp loại tổ chức, cá nhân hằng năm.

đ) Triển khai hệ thống định danh và xác thực không gian mạng quốc gia; thống nhất định danh công dân, người dùng mạng xã hội, thuê bao viễn thông và tài nguyên Internet (tên miền, địa chỉ IP…). Kiên quyết xử lý triệt để tình trạng SIM "rác", tài khoản "ảo", nặc danh; áp dụng biện pháp xác thực danh tính bắt buộc đối với người dùng mạng xã hội và cơ chế kiểm soát độ tuổi để bảo vệ trẻ em trên không gian mạng.

2. Hoàn thiện thể chế, chính sách và nâng cao hiệu lực, hiệu quả quản lý nhà nước

a) Rà soát, ban hành theo thẩm quyền hoặc đề xuất cấp có thẩm quyền sửa đổi, bổ sung, hoàn thiện, thống nhất, đồng bộ hệ thống pháp luật, cơ chế, chính sách về an ninh mạng, bảo mật thông tin, bảo vệ dữ liệu cá nhân. Đề xuất các chế tài xử lý nghiêm minh các hành vi vi phạm pháp luật trên không gian mạng.

b) Thống nhất đầu mối, phân định rõ trách nhiệm quản lý nhà nước bảo đảm hiệu lực, hiệu quả. Công an tỉnh chịu trách nhiệm trước UBND tỉnh, chủ trì quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với các hệ thống thông tin, cơ sở dữ liệu và quản lý hoạt động cung cấp sản phẩm, dịch vụ an ninh mạng đối với các hệ thống này (*trừ hệ thống thông tin, cơ sở dữ liệu quân sự và cơ yếu trong phạm vi Bộ Quốc phòng quản lý*). Văn phòng Tỉnh ủy, Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh thực hiện trách nhiệm, phạm vi quản lý về mật mã và sản phẩm mật mã theo đúng quy định tại Luật An ninh mạng năm 2025.

c) Triển khai quy hoạch và phát triển hạ tầng số, hạ tầng dữ liệu bảo đảm hiện đại, đồng bộ, an toàn; quản lý chặt chẽ hoạt động của doanh nghiệp cung cấp dịch vụ trên không gian mạng. Nâng cao trách nhiệm của các doanh nghiệp viễn thông, Internet, tài chính, ngân hàng trong việc bảo đảm an ninh hệ thống và trong công tác phối hợp với cơ quan chức năng về công tác bảo đảm an ninh mạng, bảo mật thông tin.

3. Tập trung đầu tư, hiện đại hoá hạ tầng, công nghệ và các giải pháp kỹ thuật bảo đảm an ninh mạng

a) Áp dụng đồng bộ kiến trúc bảo vệ an ninh mạng cho hạ tầng mạng Internet và hệ thống thông tin của các cơ quan, đơn vị, địa phương, doanh nghiệp trên địa bàn tỉnh. Tiếp tục khảo sát, kết nối các hệ thống thông tin quan trọng trên địa bàn tới Hệ thống phòng vệ mạng quốc gia, Nền tảng điều hành an ninh mạng quốc gia, Trung tâm An ninh mạng quốc gia. Nghiên cứu phương án xây dựng Trung tâm An ninh mạng tỉnh Lai Châu, mở rộng kết nối giám sát an ninh

mạng đến toàn bộ hệ thống thông tin, hệ thống dùng chung trên địa bàn tỉnh. Chủ động thiết lập kênh kết nối, trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an ninh mạng theo hướng dẫn của cấp trên.

b) Rà soát, kiểm tra, đánh giá định kỳ công tác bảo đảm an ninh thông tin, an ninh mạng. Tập trung phát triển giải pháp kỹ thuật bảo đảm tuyệt đối an toàn cho các hệ thống thông tin trọng yếu; tăng cường phối hợp chặt chẽ, hiệp đồng tác chiến giữa các lực lượng chuyên trách trong bảo vệ an ninh mạng.

c) Rà soát hạ tầng công nghệ thông tin theo hướng tập trung máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện an ninh mạng. Tăng cường bảo đảm an ninh kết nối, duy trì sự ổn định, thông suốt và an toàn an ninh mạng. Xây dựng hạ tầng công nghệ số hiện đại, an toàn và đồng bộ, đáp ứng yêu cầu phát triển kinh tế - xã hội và chuyển đổi số; xây dựng hệ thống bảo vệ dữ liệu và không gian mạng an toàn.

d) Bảo đảm nguồn lực tài chính bền vững cho công tác an ninh mạng. Thực hiện nghiêm quy định ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng trong nước trong các dự án đầu tư công. Bảo đảm tỉ lệ kinh phí chi cho an ninh mạng, bảo mật thông tin đạt tối thiểu 15% tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số, phù hợp với khả năng cân đối ngân sách của địa phương; đầu tư có trọng tâm, trọng điểm, tránh dàn trải, lãng phí.

4. Xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng; phát triển tiềm lực, công nghệ và nguồn nhân lực

a) Xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng vững chắc. Phát huy vai trò nòng cốt của lực lượng vũ trang nhân dân, sức mạnh tổng hợp của các doanh nghiệp công nghệ, viễn thông và các tầng lớp Nhân dân trong bảo vệ an ninh mạng. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet phải xác định rõ trách nhiệm là "tuyến đầu" trong bảo vệ an ninh mạng. Bảo đảm an toàn, an ninh mạng và chủ quyền quốc gia trên nền tảng số và không gian mạng; đảm bảo an ninh, an toàn dữ liệu hợp pháp của tổ chức, cá nhân, doanh nghiệp và chủ quyền an ninh dữ liệu quốc gia; từng bước ứng dụng công nghệ số trong chỉ huy, điều hành tác chiến của lực lượng vũ trang cũng như làm chủ công nghệ cao trong hoạt động quốc phòng, an ninh; ngăn chặn hiệu quả tội phạm trong lĩnh vực chuyển đổi số, chống lừa đảo trực tuyến.

b) Phát triển văn hóa số bảo đảm giữ gìn bản sắc dân tộc, triển khai bộ quy tắc ứng xử trên không gian mạng, giảm thiểu tác động tiêu cực của công nghệ số đối với xã hội. Đẩy mạnh đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao. Tiếp tục hoàn thiện cơ chế, chính sách thu hút, đãi ngộ cán bộ giỏi tham gia phục vụ công tác an ninh mạng trên địa bàn tỉnh.

5. Về hợp tác quốc tế trên lĩnh vực an ninh mạng

Tập trung đẩy mạnh hợp tác nghiên cứu khoa học, phát triển công nghệ với các quốc gia có trình độ khoa học và công nghệ, chuyển đổi số phát triển; phối hợp trong công tác phòng, chống và ứng phó sự cố tấn công mạng. Có chính sách mua, chuyển giao công nghệ tiên tiến phù hợp với điều kiện của tỉnh. Tăng cường phối hợp, chia sẻ thông tin tình báo, cảnh báo sớm, phòng, chống và ứng phó sự cố tấn công mạng với lực lượng chức năng các nước khác. Cử cán bộ đi đào tạo, huấn luyện chuyên sâu và tích cực tham gia các cuộc diễn tập an ninh mạng quốc tế.

IV- TỔ CHỨC THỰC HIỆN

1. Các đảng ủy trực thuộc Tỉnh ủy căn cứ chức năng, nhiệm vụ tổ chức phổ biến, quán triệt, tuyên truyền và ban hành kế hoạch cụ thể hóa thực hiện Chỉ thị số 57-CT/TW và Chương trình hành động này. Đảng ủy UBND tỉnh lãnh đạo UBND tỉnh xây dựng kế hoạch cụ thể để tổ chức thực hiện.

2. Ban Tuyên giáo và Dân vận Tỉnh ủy hướng dẫn, định hướng tuyên truyền, quán triệt Chỉ thị số 57-CT/TW và Chương trình hành động của Ban Thường vụ Tỉnh ủy.

3. Đảng ủy Công an tỉnh lãnh đạo Công an tỉnh triển khai công tác giám sát, bảo đảm an ninh mạng; các nhiệm vụ về ứng dụng sản phẩm mật mã an ninh; huy động các nguồn lực xã hội tham gia bảo vệ an ninh mạng quốc gia. Thường xuyên theo dõi, đôn đốc, kiểm tra, giám sát việc thực hiện; tham mưu Ban Thường vụ Tỉnh ủy định kỳ sơ kết, tổng kết việc thực hiện Chỉ thị số 57-CT/TW và Chương trình hành động này.

4. Đảng ủy Quân sự tỉnh lãnh đạo thực hiện công tác bảo đảm an ninh mạng, mật mã, bảo mật thông tin trong lĩnh vực quân sự, cơ yếu thuộc phạm vi quản lý.

5. Văn phòng Tỉnh ủy: Tham mưu quản lý nhà nước về mật mã *(bao gồm mật mã cơ yếu, mật mã dân sự)* và sản phẩm mật mã cơ yếu.

Nơi nhận:
- Văn phòng Trung ương Đảng,
- Các đảng ủy trực thuộc Tỉnh ủy,
- Các ban đảng tỉnh,
- Các đồng chí Tỉnh ủy viên,
- Lưu VPTU.

T/M BAN THƯỜNG VỤ
PHÓ BÍ THƯ

Sùng A Hồ