

UBND TỈNH TÂY NINH
SỞ Y TẾ

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 6020 /SYT-TCCB
V/v triển khai thực hiện
Chỉ thị số 57-CT/TU của
Ban Thường vụ Tỉnh ủy

Tây Ninh, ngày 07 tháng 6 năm 2026

Kính gửi: Thủ trưởng cơ quan, đơn vị trực thuộc Sở.

Thực hiện Chỉ thị số 57-CT/TU ngày 05/5/2026 của Ban Thường vụ Tỉnh ủy về việc thực hiện Chỉ thị số 57-CT/TW 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.

Sở Y tế sao gửi Thủ trưởng cơ quan, đơn vị về Chỉ thị số 57-CT/TU của Ban Thường vụ Tỉnh ủy nêu trên (*đính kèm*), đồng thời đề nghị Thủ trưởng cơ quan, đơn vị phối hợp cấp ủy chi đảng bộ trực thuộc tổ chức quán triệt, triển khai thực hiện nghiêm túc, hiệu quả Chỉ thị số 57-CT/TW và Chương trình hành động này; đồng thời, xây dựng chương trình, kế hoạch thực hiện cụ thể, sát với tình hình thực tế của cơ quan, đơn vị.

Nơi nhận:

- Như trên;
- Đảng ủy Sở Y tế (b/c);
- BGĐ Sở Y tế;
- Các chi đảng bộ trực thuộc;
- Các phòng chuyên môn, nghiệp vụ Sở;
- Lưu: VT, TCCB.

GIÁM ĐỐC



Đỗ Hồng Sơn



Tỉnh ủy Tây Ninh
07/05/2026 08:56:14

TỈNH ỦY TÂY NINH

*

Số 62-CTr/TU

ĐẢNG CỘNG SẢN VIỆT NAM

Tây Ninh, ngày 05 tháng 5 năm 2026

CHƯƠNG TRÌNH HÀNH ĐỘNG
CỦA BAN THƯỜNG VỤ TỈNH ỦY
thực hiện Chỉ thị số 57-CT/TW 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 (*Chỉ thị số 57-CT/TW*); Ban Thường vụ Tỉnh ủy ban hành Chương trình hành động thực hiện như sau:

I. ĐÁNH GIÁ TÌNH HÌNH

- Thời gian qua, việc triển khai thực hiện các chủ trương, chỉ thị, nghị quyết, kết luận của Bộ Chính trị, Ban Bí thư về tăng cường bảo đảm an ninh mạng, an toàn thông tin và bảo vệ dữ liệu trong hệ thống chính trị trên địa bàn tỉnh đã được các cấp ủy, tổ chức đảng, chính quyền, cơ quan, đơn vị quan tâm lãnh đạo, chỉ đạo và tổ chức thực hiện nghiêm túc; nhận thức về tầm quan trọng của an ninh mạng được nâng lên; hành lang pháp lý từng bước được hoàn thiện; năng lực kỹ thuật bảo đảm an ninh mạng của các cơ quan trọng yếu được tăng cường.

- Công tác xây dựng, hoàn thiện cơ chế, chính sách, kế hoạch về bảo đảm an toàn thông tin, an ninh mạng được chú trọng; nhiều chương trình, kế hoạch về chuyển đổi số, bảo đảm an toàn thông tin mạng đã được ban hành và triển khai đồng bộ trong toàn hệ thống chính trị trên địa bàn tỉnh. Việc đầu tư hạ tầng công nghệ thông tin, trung tâm tích hợp dữ liệu tỉnh, hệ thống thông tin dùng chung và các nền tảng số phục vụ hoạt động của hệ thống chính trị từng bước được tăng cường, góp phần nâng cao hiệu quả quản lý, điều hành và phục vụ người dân, doanh nghiệp, tổ chức trong hệ thống chính trị sau sắp xếp, sáp nhập, điều chỉnh địa giới hành chính và thực hiện chính quyền địa phương 2 cấp.

- Việc đào tạo, bồi dưỡng nguồn nhân lực về an toàn thông tin được quan tâm; đội ngũ cán bộ chuyên trách và bán chuyên trách về công nghệ thông tin, an toàn thông tin từng bước được nâng cao trình độ chuyên môn, đáp ứng yêu

cầu nhiệm vụ. Theo Kế hoạch của Ban Thường vụ Tỉnh ủy¹, 100% nhân sự chuyên trách công nghệ thông tin và an toàn thông tin tại các sở, ban, ngành và địa phương được đào tạo, bồi dưỡng hằng năm nhằm nâng cao năng lực bảo đảm an toàn hệ thống thông tin. Ngoài ra, các cơ quan, đơn vị từng bước nâng cao nhận thức về bảo đảm an ninh mạng, tăng cường kiểm tra, rà soát, đánh giá các hệ thống thông tin, chủ động phát hiện, khắc phục kịp thời các lỗ hổng bảo mật và xây dựng phương án ứng phó sự cố an ninh mạng, an toàn thông tin. Tỉnh Tây Ninh đã triển khai các biện pháp nhằm bảo vệ các hệ thống thông tin quan trọng, chuyển từ trạng thái bị động sang chủ động phòng ngừa, phát hiện và xử lý các nguy cơ tấn công mạng.

- *Bên cạnh những kết quả đạt được, công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ dữ liệu trong hệ thống chính trị trên địa bàn tỉnh vẫn còn một số hạn chế:* Nhận thức về an ninh mạng ở một bộ phận lãnh đạo, cán bộ, đảng viên và nhân dân trong tỉnh chưa đầy đủ và sâu sắc; tình hình tấn công mạng ngày càng gia tăng với phương thức, thủ đoạn ngày càng tinh vi; nguồn nhân lực chuyên sâu về an toàn thông tin còn thiếu; việc đầu tư trang thiết bị, giải pháp kỹ thuật bảo mật chưa thật sự đồng bộ, tập trung; nguy cơ tấn công mạng, lộ lọt thông tin, dữ liệu vẫn tiềm ẩn nhiều rủi ro trong bối cảnh chuyển đổi số diễn ra mạnh mẽ trên phạm vi cả nước và tại tỉnh.

- Dự báo tình hình an ninh mạng, bảo mật thông tin, an ninh dữ liệu trên thế giới, trong nước nói chung và trên địa bàn tỉnh nói riêng thời gian tới có nhiều diễn biến phức tạp, khó lường. Trong bối cảnh dữ liệu trở thành tài nguyên chiến lược, trí tuệ nhân tạo phát triển nhanh chóng, không gian mạng trở thành không gian tác chiến mới, công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo mật thông tin không chỉ là nhiệm vụ kỹ thuật mà là vấn đề an ninh quốc gia, chủ quyền quốc gia, ổn định chính trị, xã hội và năng lực cạnh tranh quốc gia. Công cuộc chuyển đổi số trên địa bàn tỉnh đối mặt với những thách thức, an ninh mạng, an toàn thông tin, trật tự, an toàn xã hội, ảnh hưởng, đe dọa an ninh quốc gia,..., đặt ra yêu cầu cấp bách đối với công tác này trong giai đoạn mới.

II. NHIỆM VỤ, GIẢI PHÁP TRỌNG TÂM

1. Tăng cường sự lãnh đạo, chỉ đạo của cấp ủy, chính quyền các cấp đối với công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ dữ liệu; xác định đây là nhiệm vụ trọng tâm, thường xuyên trong quá trình xây dựng chính quyền số, phát triển kinh tế số và xã hội số trên địa bàn tỉnh

¹ Kế hoạch số 35-KH/TU, ngày 12/02/2026 của Ban Thường vụ Tỉnh ủy thực hiện Nghị quyết số 57-NQ/TW của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.

- Quán triệt quan điểm bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu là nhiệm vụ trọng yếu, thường xuyên, cấp bách của cả hệ thống chính trị và toàn dân đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý tập trung, thống nhất của Nhà nước; phát huy vai trò nòng cốt của lực lượng Công an nhân dân, Quân đội nhân dân; 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.

- Bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu gắn chặt với quá trình chuyên đổi số, xây dựng chính quyền số, phát triển kinh tế số và xã hội số; đồng thời, bảo vệ vững chắc chủ quyền, lợi ích quốc gia, giữ vững ổn định chính trị, trật tự, an toàn xã hội trên không gian mạng. Xây dựng hệ sinh thái bảo đảm an ninh mạng đồng bộ, hiện đại, trong đó chú trọng hoàn thiện thể chế, cơ chế phối hợp; đầu tư hạ tầng kỹ thuật, công nghệ bảo mật; phát triển nguồn nhân lực chất lượng cao; tăng cường hợp tác, chia sẻ thông tin, nâng cao năng lực giám sát, cảnh báo sớm và ứng phó, khắc phục sự cố an ninh mạng.

- Quán triệt phương châm “*tự chủ, tự lực, tự cường*” trong xây dựng tiềm lực an ninh mạng; tập trung phát triển, khai thác và sử dụng hiệu quả hệ sinh thái sản phẩm, dịch vụ an ninh mạng Việt Nam; ưu tiên làm chủ công nghệ lõi, các giải pháp bảo mật tiên tiến; đẩy mạnh ứng dụng trí tuệ nhân tạo và các công nghệ mới trong lĩnh vực an ninh mạng, coi đây là nhiệm vụ chiến lược nhằm bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu tại tỉnh, góp phần bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng. Đồng thời, nghiên cứu, áp dụng các cơ chế, chính sách đột phá, đặc thù và ưu đãi trong lĩnh vực khoa học, công nghệ và đổi mới sáng tạo để thúc đẩy phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng và an ninh dữ liệu.

- 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, triển khai và vận hành các hệ thống thông tin. Kiên quyết không đưa vào khai thác, sử dụng đối với các hệ thống chưa bảo đảm yêu cầu về an toàn, an ninh mạng. Thường xuyên tổ chức rà soát, kiểm tra, đánh giá mức độ an toàn, an ninh mạng đối với các hệ thống công nghệ thông tin. Việc thu thập, quản lý, lưu trữ và khai thác dữ liệu số phải được bảo vệ ở mức độ cao nhất; tuyệt đối không để xảy ra lộ, lọt bí mật nhà nước, dữ liệu nhạy cảm, kể cả trong quá trình thử nghiệm, vận hành thử hoặc phát triển hệ thống.

- Chuyển dịch tư duy bảo đảm an ninh mạng từ “*phòng thủ bị động*” sang “*phòng thủ chủ động*”, “*phòng thủ tích cực*”, từng bước xây dựng thế trận an ninh mạng chủ động, toàn diện. Chủ động nhận diện, dự báo sớm các nguy cơ, thách thức đối với an ninh mạng, bảo mật thông tin và an ninh dữ liệu; kịp thời triển khai các biện pháp phòng ngừa, phát hiện và xử lý từ sớm, từ xa; sẵn sàng

áp dụng các biện pháp phòng vệ phù hợp nhằm răn đe, vô hiệu hóa các nguy cơ, bảo vệ lợi ích quốc gia, dân tộc.

- 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 và bảo vệ bí mật nhà nước tại địa phương, cơ quan, đơn vị mình. Kết quả thực hiện nhiệm vụ này được xác định là một trong những tiêu chí quan trọng trong đánh giá, xếp loại hằng năm đối với tổ chức, cán bộ, đảng viên, công chức, viên chức và người lao động.

- Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, giáo dục kiến thức và kỹ năng về an ninh mạng; từng bước đưa nội dung này vào chương trình giáo dục trong hệ thống giáo dục và các chương trình tuyên truyền, phổ biến kiến thức số, góp phần hình thành “thế hệ công dân số” văn minh, tuân thủ pháp luật. Triển khai các cơ chế đánh giá, nâng cao mức độ tin nhiệm trên không gian mạng; tăng cường liên kết, hợp tác giữa các cơ quan, tổ chức nhằm xây dựng không gian mạng an toàn, lành mạnh, tin cậy, thúc đẩy các giá trị nhân văn và nâng cao ý thức trách nhiệm bảo đảm an ninh mạng cho mọi người dùng.

- Đẩy mạnh phong trào toàn dân bảo vệ an ninh mạng; phát huy trách nhiệm xã hội của các cơ quan báo chí, truyền thông và người có uy tín trong việc định hướng dư luận, lan tỏa thông tin tích cực, đấu tranh phản bác các thông tin xấu độc trên không gian mạng. Đồng thời, chú trọng đào tạo, bồi dưỡng, nâng cao năng lực chuyên môn, kỹ năng nghiệp vụ cho lực lượng chuyên trách về an ninh mạng, đáp ứng yêu cầu nhiệm vụ trong tình hình mới.

- Triển khai đồng bộ hệ thống định danh và xác thực điện tử trên không gian mạng, bảo đảm thống nhất trong quản lý định danh công dân, người dùng mạng xã hội, thuê bao viễn thông và tài nguyên Internet (*tên miền, địa chỉ IP, ...*). Tăng cường quản lý, kiểm soát thông tin thuê bao; kiên quyết xử lý triệt để tình trạng SIM “rác”, tài khoản “ảo”, tài khoản nặc danh trên không gian mạng. Áp dụng các biện pháp xác thực danh tính bắt buộc đối với người dùng các nền tảng mạng xã hội; đồng thời, triển khai cơ chế kiểm soát độ tuổi, bảo vệ trẻ em trên không gian mạng, góp phần xây dựng môi trường số an toàn, lành mạnh.

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

- rà soát, hoàn thiện hệ thống văn bản quy phạm pháp luật, cơ chế, chính sách về bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu phù hợp với yêu cầu thực tiễn và tiến trình chuyển đổi số. Xây dựng, ban hành và tổ chức thực hiện đồng bộ các quy chế, quy định về quản lý, vận hành, khai thác,

chia sẻ và bảo vệ dữ liệu trong các cơ quan thuộc hệ thống chính trị trên địa bàn tỉnh.

- Tăng cường hiệu lực, hiệu quả quản lý nhà nước về an ninh mạng; xác định rõ trách nhiệm của các cơ quan, đơn vị, địa phương trong công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ bí mật nhà nước trên không gian mạng. Đẩy mạnh công tác thanh tra, kiểm tra, giám sát việc chấp hành pháp luật, kịp thời phát hiện, xử lý nghiêm các hành vi vi phạm quy định về an ninh mạng, an toàn thông tin và bảo vệ dữ liệu.

- Thống nhất đầu mối quản lý, phân định rõ trách nhiệm trong công tác quản lý nhà nước nhằm bảo đảm hiệu lực, hiệu quả. Trong đó:

+ *Về an ninh mạng*: Công an tỉnh chịu trách nhiệm trước Tỉnh ủy, Ban Thường vụ Tỉnh ủy, Ủy ban nhân dân tỉnh chủ trì quản lý nhà nước về an ninh mạng, bảo mật thông tin và an ninh dữ liệu đối với các hệ thống thông tin, cơ sở dữ liệu của toàn hệ thống chính trị trên địa bàn tỉnh. Đồng thời, thực hiện quản lý hoạt động cung cấp sản phẩm, dịch vụ an ninh mạng đối với các hệ thống này (*trừ các hệ thống thông tin, cơ sở dữ liệu quân sự và cơ yếu thuộc phạm vi quản lý của Bộ Chỉ huy Quân sự tỉnh*).

+ Về mật mã và sản phẩm mật mã: Công an tỉnh và Bộ Chỉ huy Quân sự tỉnh thực hiện chức năng, nhiệm vụ và phạm vi quản lý nhà nước theo quy định của Luật An ninh mạng năm 2025 và các quy định pháp luật có liên quan.

- Quy hoạch, phát triển hạ tầng số, hạ tầng dữ liệu bảo đảm hiện đại, đồng bộ, an toàn, đáp ứng yêu cầu chuyển đổi số và phát triển kinh tế số, xã hội số. Thực hiện nghiêm các quy định của pháp luật, bảo đảm hồ sơ thiết kế hệ thống thông tin, các dự án công nghệ thông tin và dự án chuyển đổi số phải có cấu phần bảo đảm an ninh mạng, an toàn thông tin được thẩm định, phê duyệt trước khi triển khai đầu tư, xây dựng và đưa vào vận hành.

- Xây dựng và áp dụng bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng làm cơ sở theo dõi, đánh giá, xếp hạng mức độ bảo đảm an ninh mạng của các cơ quan, đơn vị, địa phương. Đồng thời, hoàn thiện cơ chế trao đổi, chia sẻ thông tin, cảnh báo sớm và quy trình phối hợp ứng cứu sự cố an ninh mạng giữa các cơ quan, tổ chức trong và ngoài tỉnh, góp phần nâng cao hiệu quả phòng ngừa, phát hiện và xử lý các sự cố trên không gian mạng.

- Hoàn thiện hành lang pháp lý nhằm quản lý chặt chẽ hoạt động của các doanh nghiệp cung cấp dịch vụ trên không gian mạng, bao gồm cả các dịch vụ xuyên biên giới. Quy định rõ trách nhiệm của các doanh nghiệp viễn thông, Internet, tài chính, ngân hàng trong việc bảo đảm an ninh, an toàn hệ thống thông tin và phối hợp chặt chẽ với các cơ quan chức năng trong công tác phòng ngừa, phát hiện, đấu tranh, xử lý vi phạm pháp luật trên không gian mạng.

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

- Ưu tiên đầu tư, nâng cấp hạ tầng kỹ thuật, nền tảng công nghệ và các giải pháp bảo mật nhằm nâng cao năng lực bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu đối với các hệ thống thông tin, cơ sở dữ liệu quan trọng của tỉnh. Xây dựng Trung tâm An ninh mạng tỉnh thực hiện giám sát, cảnh báo sớm, phát hiện và ứng phó sự cố an ninh mạng hoạt động tập trung, đồng bộ, kết nối với các hệ thống giám sát, cảnh báo của Trung tâm An ninh mạng quốc gia.

- Đẩy mạnh triển khai các giải pháp kỹ thuật tiên tiến, ứng dụng trí tuệ nhân tạo, phân tích dữ liệu lớn và các công nghệ mới trong công tác giám sát, phát hiện, phòng ngừa và xử lý các nguy cơ, sự cố an ninh mạng. Đồng thời, bảo đảm các hệ thống thông tin quan trọng được phân loại, xác định cấp độ an toàn thông tin và áp dụng đầy đủ các biện pháp bảo vệ theo quy định.

- Bảo đảm nguồn lực tài chính ổn định, bền vững cho công tác bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu. Thực hiện nghiêm quy định ưu tiên sử dụng các sản phẩm, giải pháp an ninh mạng do Việt Nam nghiên cứu, phát triển trong các dự án đầu tư công. Bảo đảm tỷ lệ kinh phí chi cho an ninh mạng, bảo mật thông tin đạt **tối thiểu 15%** tổng kinh phí triển khai các kế hoạch, dự án ứng dụng công nghệ thông tin và chuyển đổi số; đồng thời, tổ chức đầu tư có trọng tâm, trọng điểm, tránh dàn trải, lãng phí, nâng cao hiệu quả sử dụng nguồn lực.

- Tăng cường kiểm tra, đánh giá an toàn thông tin mạng; thường xuyên rà soát, khắc phục các lỗ hổng, điểm yếu bảo mật; bảo đảm các hệ thống thông tin được vận hành an toàn, ổn định, liên tục, đáp ứng yêu cầu phục vụ công tác quản lý, điều hành của các cơ quan trong hệ thống chính trị và nhu cầu của người dân, doanh nghiệp.

- Rà soát, điều chỉnh quy hoạch hạ tầng công nghệ thông tin theo hướng tập trung hệ thống máy chủ, dữ liệu tại trung tâm dữ liệu đạt tiêu chuẩn, bảo đảm yêu cầu về an ninh mạng, an toàn thông tin. Tăng cường các biện pháp bảo đảm an ninh kết nối, duy trì sự ổn định, thông suốt và an toàn của các luồng dữ liệu quan trọng; bảo đảm khả năng kết nối trong mọi tình huống, kể cả khi xảy ra sự cố nghiêm trọng, thảm họa hoặc các tình huống khẩn cấp như thiên tai, dịch bệnh, chiến tranh.

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

- Xây dựng thể trận an ninh nhân dân gắn với thể trận quốc phòng toàn

dân trên không gian mạng vững chắc. Phát huy vai trò nòng cốt của lực lượng vũ trang nhân dân, đồng thời huy động sức mạnh tổng hợp của các doanh nghiệp công nghệ, viễn thông và các tầng lớp nhân dân trong công tác bảo đảm an ninh mạng. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet cần xác định rõ trách nhiệm là “*tuyến đầu*” trong bảo vệ an ninh mạng, chủ động phối hợp với các cơ quan chức năng trong việc phòng ngừa, phát hiện, ngăn chặn và xử lý các hành vi vi phạm pháp luật trên không gian mạng.

- Tập trung nguồn lực đầu tư ưu tiên ứng dụng các sản phẩm an ninh mạng “*Made in Vietnam*”. Trong đó, chú trọng áp dụng các sản phẩm cốt lõi, nền tảng như: Giải pháp tường lửa, phòng chống mã độc, bảo vệ thiết bị đầu cuối, nền tảng điện toán đám mây và hệ điều hành chuyên dụng phục vụ các hệ thống thông tin quan trọng. Có cơ chế, chính sách hỗ trợ, thu hút các doanh nghiệp công nghệ tham gia phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng.

- Đẩy mạnh đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao, đáp ứng yêu cầu nhiệm vụ trong tình hình mới. Tăng cường liên kết với các cơ sở đào tạo có uy tín, chất lượng cao trong công tác đào tạo, bồi dưỡng và huấn luyện thực hành, thực chiến về an ninh mạng. Đồng thời, tiếp tục hoàn thiện cơ chế, chính sách thu hút, trọng dụng và đãi ngộ chuyên gia, nhân tài trong lĩnh vực an ninh mạng tham gia phục vụ nhiệm vụ bảo đảm an ninh mạng.

5. Tăng cường phối hợp và hợp tác quốc tế trong lĩnh vực an ninh mạng

- Chủ động mở rộng, tăng cường hợp tác với các địa phương, khu vực trong nước và quốc tế trong lĩnh vực an ninh mạng, an toàn thông tin, an ninh dữ liệu phù hợp với đường lối, chủ trương đối ngoại của Đảng, chính sách, pháp luật của Nhà nước và tình hình thực tiễn của địa phương; tranh thủ nguồn lực, kinh nghiệm, công nghệ tiên tiến của địa phương, khu vực trong nước, của các quốc gia, tổ chức quốc tế, nhằm nâng cao năng lực bảo đảm an ninh mạng trên địa bàn tỉnh.

- Tăng cường trao đổi thông tin, chia sẻ kinh nghiệm, hợp tác đào tạo, huấn luyện và chuyển giao công nghệ trong lĩnh vực an ninh mạng; thúc đẩy hợp tác trong phòng ngừa, phát hiện, điều tra, xử lý tội phạm sử dụng công nghệ cao và tội phạm trên không gian mạng.

- Đẩy mạnh tham gia các diễn đàn, cơ chế hợp tác khu vực và quốc tế về an ninh mạng; xây dựng cơ chế phối hợp, chia sẻ thông tin cảnh báo sớm, hỗ trợ ứng cứu sự cố an ninh mạng xuyên biên giới, góp phần bảo vệ chủ quyền quốc gia, lợi ích quốc gia trên không gian mạng.

- Thiết lập cơ chế phối hợp giữa Công an tỉnh, Sở Khoa học và Công nghệ, Bộ Chỉ huy Quân sự tỉnh và các cơ quan, đơn vị có liên quan trong tham mưu

thực hiện các nhiệm vụ bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh.

III. TỔ CHỨC THỰC HIỆN

1. Các đảng ủy trực thuộc Tỉnh ủy; các cơ quan tham mưu, giúp việc Tỉnh ủy; các sở, ngành, Mặt trận Tổ quốc và tổ chức chính trị - xã hội tỉnh có trách nhiệm tổ chức quán triệt, triển khai thực hiện nghiêm túc, hiệu quả Chỉ thị số 57-CT/TW và Chương trình hành động này; đồng thời, xây dựng chương trình, kế hoạch thực hiện cụ thể, sát với tình hình thực tế của địa phương, cơ quan, đơn vị; định kỳ kiểm tra, đánh giá kết quả thực hiện và báo cáo Ban Thường vụ Tỉnh ủy theo quy định (*qua Đảng ủy Công an tỉnh*).

2. Đảng ủy Ủy ban nhân dân tỉnh

- Lãnh đạo Ủy ban nhân dân tỉnh xây dựng chương trình, kế hoạch cụ thể hóa các giải pháp phù hợp; đảm bảo thực hiện hiệu quả Chỉ thị số 57-CT/TW và Chương trình hành động này.

- Chỉ đạo các cơ quan liên quan nghiên cứu xây dựng, ban hành cơ chế, chính sách đặc thù, ưu đãi vượt trội để thu hút, giữ chân các chuyên gia, người tài an ninh mạng, bổ sung nguồn nhân lực chất lượng cao phục vụ hiệu quả quá trình chuyển đổi số, phát triển kinh tế số và xây dựng xã hội số trên địa bàn tỉnh.

3. Đảng ủy Công an tỉnh

- Chịu trách nhiệm về thực hiện thống nhất quản lý nhà nước về an ninh mạng, an toàn thông tin, an ninh dữ liệu (*trừ lĩnh vực quân sự, cơ yếu*).

- Chủ trì, phối hợp đẩy mạnh kết nối, sử dụng dữ liệu từ cơ sở dữ liệu quốc gia về dân cư để áp dụng thống nhất định danh trên không gian mạng một cách toàn diện. Tập trung chỉ đạo xử lý dứt điểm tình trạng SIM “rác”, tài khoản “ảo”, từng bước thiết lập trật tự, kỷ cương trong quản lý người dùng mạng xã hội; đồng thời bảo đảm các yêu cầu về bảo vệ an ninh mạng quốc gia, bảo vệ dữ liệu cá nhân và bảo vệ trẻ em trên không gian mạng.

- Chủ trì phối hợp với các cơ quan, đơn vị liên quan trong công tác triển khai các giải pháp kỹ thuật, giám sát, cảnh báo sớm và hỗ trợ ứng cứu sự cố an toàn thông tin đối với các hệ thống thông tin của tỉnh.

4. Đảng ủy Quân sự tỉnh

Chịu trách nhiệm toàn diện trước Ban Thường vụ Tỉnh ủy về 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, phụ trách.

5. Ban Tuyên giáo và Dân vận Tỉnh ủy

Chủ trì hướng dẫn, định hướng công tác tuyên truyền, phổ biến, quán triệt sâu rộng trong cán bộ, đảng viên và nhân dân trên địa bàn tỉnh nội dung về Chỉ thị số 57-CT/TW và Chương trình hành động này, gắn với các chủ trương, quy định của Đảng, chính sách, pháp luật của Nhà nước về đảm bảo an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị, góp phần nâng cao nhận thức, trách nhiệm của các cấp, ngành, cơ quan, tổ chức và người dân trong công tác bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu.

6. Giao Đảng ủy Công an tỉnh chủ trì, phối hợp với Đảng ủy Quân sự tỉnh, các cơ quan liên quan theo dõi, giám sát, kiểm tra, đôn đốc việc triển khai thực hiện Chỉ thị số 57-CT/TW và Chương trình hành động này; kịp thời tham mưu, đề xuất giải quyết những vấn đề, khó khăn, vướng mắc phát sinh; định kỳ hoặc theo yêu cầu của Trung ương thực hiện sơ kết, tổng kết, báo cáo kết quả thực hiện theo quy định.

Nơi nhận:

- Văn phòng Trung ương Đảng,
- Đảng ủy Công an Trung ương,
- Quân ủy Trung ương,
- Các đồng chí Tỉnh ủy viên,
- Các cơ quan tham mưu, giúp việc Tỉnh ủy,
- Các đảng ủy trực thuộc Tỉnh ủy,
- Các sở, ngành, MTTQ và tổ chức CT-XH tỉnh,
- Chánh, Phó Chánh Văn phòng Tỉnh ủy (P),
- Phòng TH, CDS - CY Văn phòng Tỉnh ủy,
- Lưu Văn phòng Tỉnh ủy.

T/M BAN THƯỜNG VỤ
PHÓ BÍ THƯ



Nguyễn Mạnh Hùng

Nguyễn Mạnh Hùng