Số và ký hiệu: 29-CTr/TU
Ký bởi: Tỉnh ủy Lâm Đồng
Thời gian ký: 29/05/2026 15:40:11

TỈNH ỦY LÂM ĐỒNG * Số 29 -CTr/TU	ĐẢNG CỘNG SẢN VIỆT NAM *Lâm Đồng, ngày 29 tháng 5 năm 2026*

CHƯƠNG TRÌNH HÀNH ĐỘNG
thực hiện Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư Trung ương Đảng 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 Trung ương Đảng về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị *(viết tắt là Chỉ thị số 57-CT/TW)*; Ban Thường vụ Tỉnh ủy ban hành Chương trình hành động triển khai thực hiện Chỉ thị số 57-CT/TW, như sau:

I- MỤC ĐÍCH, YÊU CẦU

1. Quán triệt, triển khai thực hiện đầy đủ, nghiêm túc Chỉ thị số 57-CT/TW, tạo sự thống nhất trong nhận thức và hành động của các cấp ủy, tổ chức đảng, chính quyền, Mặt trận Tổ quốc, các tổ chức chính trị - xã hội và Nhân dân trong công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị.

2. Xác định rõ nhiệm vụ, giải pháp trọng tâm để triển khai đồng bộ, hiệu quả Chỉ thị số 57-CT/TW. Phát huy vai trò, trách nhiệm của cả hệ thống chính trị trong lãnh đạo, chỉ đạo và tổ chức thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu gắn với nhiệm vụ chuyển đổi số, xây dựng chính quyền điện tử, chính quyền số của tỉnh.

3. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, xử lý kịp thời các nguy cơ, thách thức, hành vi xâm phạm an ninh quốc gia, trật tự an toàn xã hội trên không gian mạng, không để bị động, bất ngờ trong mọi tình huống.

4. Các cấp ủy, tổ chức đảng, chính quyền, cơ quan, đơn vị, địa phương và người đứng đầu lãnh đạo, chỉ đạo triển khai thực hiện các nội dung, nhiệm vụ, giải pháp bảo đảm đồng bộ, toàn diện, có trọng tâm, trọng điểm với lộ trình phù hợp, hiệu quả.

5. Thường xuyên theo dõi, kiểm tra, giám sát việc triển khai thực hiện, kịp thời sơ kết, tổng kết, điều chỉnh các nhiệm vụ, giải pháp phù hợp với tình hình thực tiễn và các chủ trương mới của Trung ương.

II- NHIỆM VỤ, GIẢI PHÁP TRỌNG TÂM*

1. Tăng cường sự lãnh đạo của 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

---

* Các cấp ủy, tổ chức đảng, chính quyền, cơ quan, đơn vị có liên quan thường xuyên triển khai thực hiện các nhiệm vụ, giải pháp trọng tâm.

- Quán triệt sâu sắc quan điểm bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ trọng yếu, thường xuyên, cấp bách; là trách nhiệm 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. Lực lượng Công an nhân dân, Quân đội nhân dân đóng vai trò chủ chốt. 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.

- Chuyển dịch tư duy chiến lược từ "phòng thủ bị động" sang "phòng thủ chủ động", "phòng thủ tích cực", xây dựng "thế trận an ninh mạng chủ động, toàn diện"; những nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an ninh dữ liệu phải được nhận diện và xử lý từ sớm, từ xa; chủ động xây dựng kịch bản ứng phó đối với các tình huống tấn công mạng có thể xảy ra, nhất là tấn công có chủ đích vào hạ tầng trọng yếu như hệ thống ngân hàng, tài chính, năng lượng, viễn thông, giao thông,... Định kỳ tổ chức tập huấn, diễn tập ứng cứu sự cố an ninh mạng; sẵn sàng có các biện pháp phòng vệ tương xứng để răn đe, vô hiệu hóa các nguy cơ, bảo vệ lợi ích quốc gia - dân tộc.

- 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, coi đây là những nhiệm vụ chiến lược để bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng. Áp dụng cơ chế đột phá, đặc thù, ưu đãi nhất trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo để phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng, 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, vận hành hệ thống thông tin. Hệ thống chưa bảo đảm an toàn, an ninh thì kiên quyết chưa đưa vào sử dụng. 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, mất bí mật nhà nước, dữ liệu nhạy cảm, kể cả trong quá trình thử nghiệm.

- Người đứng đầu cấp ủy, chính quyền, cơ quan, đơn vị 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 địa phương, đơn vị mình. Kết quả công tác này là một trong những tiêu chí quan trọng để đánh giá, xếp loại tổ chức, cán bộ, đảng viên, công chức, viên chức và người lao động hằng năm.

- Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, giáo dục kiến thức, kỹ năng an ninh mạng; triển khai các chuyên đề trong Phong trào "Bình dân học vụ số" để xây dựng "thế hệ công dân số" văn minh, tuân thủ pháp luật. Triển khai

đánh giá tín nhiệm mạng, phát triển cơ chế liên kết và hợp tác nhằm xây dựng một không gian mạng an toàn, tin cậy, thúc đẩy các giá trị nhân văn và nâng cao ý thức trách nhiệm bảo đảm an ninh không gian mạng đến mọi người dùng; phát động phong trào toàn dân bảo vệ an ninh mạng.

Triển khai các giải pháp đồng bộ, "đa tầng, đa lớp, đa chiều", chuyển từ "phòng thủ, đối phó" sang "chủ động tấn công, dẫn dắt và hiệp đồng chặt chẽ"; kết hợp chặt chẽ giữa đấu tranh, xử lý và động viên, khen thưởng; kết hợp giữa công nghệ, pháp luật, tuyên truyền và sự tham gia, vào cuộc của toàn dân; phát huy trách nhiệm xã hội của cơ quan báo chí và người có uy tín trong việc định hướng dư luận, lan tỏa thông tin tích cực và đấu tranh với các thông tin xấu độc. Triển khai các cơ chế phối hợp giữa các cơ quan, ban, ngành, địa phương kết hợp với các đơn vị nghiệp vụ thuộc Bộ Công an trong công tác đề nghị các nền tảng mạng xã hội phải tuân thủ nghiêm túc pháp luật Việt Nam, gỡ bỏ thông tin vi phạm trong thời gian ngắn nhất. Tập trung đào tạo, nâng cao năng lực, kỹ năng của lực lượng chuyên trách về an ninh mạng.

- 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 theo quy định của pháp luật và hướng dẫn của cơ quan có thẩm quyền.

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

- Khẩn trương rà soát, báo cáo, đề xuất 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, dữ liệu quốc gia, tiêu chuẩn, quy chuẩn kỹ thuật. Xây dựng chế tài xử lý nghiêm minh các hành vi vi phạm pháp luật trên không gian mạng.

- Thống nhất đầu mối, phân định rõ trách nhiệm quản lý nhà nước bảo đảm hiệu lực, hiệu quả. Trong đó chủ trì triển khai công tác 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 của toàn hệ thống chính trị; phối hợp với các đơn vị thuộc Bộ Công an 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)*. Triển khai thực hiện trách nhiệm, phạm vi quản lý sản phẩm mật mã theo đúng quy định tại Luật An ninh mạng năm 2025.

- Triển khai thực hiện Quy hoạch và phát triển hạ tầng số, hạ tầng dữ liệu quốc gia trên địa bàn tỉnh bảo đảm đồng bộ, an toàn. Thực hiện nghiêm quy định

pháp luật yêu cầu hồ sơ thiết kế hệ thống thông tin, dự án chuyển đổi số phải có cấu phần an ninh mạng được thẩm định, phê duyệt trước khi đầu tư xây dựng.

- Triển khai thực hiện Khung quản trị rủi ro an ninh mạng quốc gia theo tiêu chuẩn quốc tế; chuyển đổi tư duy từ quản lý kỹ thuật thuần tuý sang quản trị rủi ro toàn diện nhằm tăng tính chủ động phân bổ nguồn lực và giảm thiểu tổn thất. Triển khai áp dụng Bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng để xếp hạng đối với các tổ chức, cơ quan, đơn vị, địa phương. Hoàn thiện cơ chế trao đổi, chia sẻ thông tin và quy trình phối hợp ứng cứu sự cố giữa các cơ quan, tổ chức trong nước và ngoài địa phương có liên quan.

- Báo cáo, đề xuất trong xây dựng, hoàn thiện hành lang pháp lý quản lý chặt chẽ hoạt động của các doanh nghiệp cung cấp dịch vụ trên không gian mạng *(bao gồm cả 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 hệ thống và phối hợp với cơ quan chức năng *(Bộ Công an, Bộ Quốc phòng)*; thiết lập cơ chế kết nối kỹ thuật, cung cấp dữ liệu, chứng cứ điện tử nhanh chóng, kịp thời, bảo đảm "đúng, đủ, sạch, sống" để phục vụ công tác điều tra, xử lý tội phạm và bảo vệ chủ quyền quốc gia; đơn giản hóa thủ tục hành chính trong các tình huống khẩn cấp về an ninh mạng.

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

- Triển khai ứng dụng các giải pháp mật mã tiên tiến, mật mã kháng lượng tử nhằm nâng cao năng lực bảo vệ bí mật nhà nước, dữ liệu quan trọng và hệ thống thông tin trọng yếu, chủ động ứng phó nguy cơ mất an toàn thông tin và tấn công mạng trong bối cảnh phát triển công nghệ tính toán lượng tử; làm chủ các công nghệ lõi chiến lược như công nghệ mật mã, thiết kế và sản xuất chip bảo mật "Make in Vietnam"; khuyến khích xã hội hóa đối với công tác phát triển, ứng dụng sản phẩm mật mã dân sự để bảo mật thông tin.

- Phối hợp trong xây dựng kiến trúc bảo vệ an ninh mạng quốc gia đồng bộ, thống nhất, đa lớp hỗ trợ bảo vệ hệ thống thông tin của các cơ quan, đơn vị, địa phương. Trong đó, tập trung phối hợp triển khai, vận hành hiệu quả Hệ thống phòng vệ mạng quốc gia và các nền tảng số dùng chung quốc gia chuyên ngành an ninh mạng là nền tảng dùng chung trong Khung kiến trúc tổng thể quốc gia số nhằm bảo vệ an ninh mạng cho các hệ thống thông tin, tài nguyên trọng yếu trên môi trường Internet của các cơ quan, đơn vị, địa phương, doanh nghiệp. Triển khai đấu nối, phát huy tối đa kết quả giám sát, phân tích hệ thống thông tin của địa phương từ Trung tâm An ninh mạng quốc gia thuộc Bộ Công an. Triển khai xây dựng, nâng cấp trung tâm an ninh mạng tại địa phương, trang bị các phương tiện, thiết bị, kỹ thuật,... quy định tại danh mục thiết bị tối thiểu cần có tại các trung tâm an ninh mạng do Bộ Công an ban hành.

Mở rộng kết nối giám sát an ninh mạng đến toàn bộ cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành, hệ thống thông tin, hệ thống dùng chung của toàn hệ thống chính trị. Đôn đốc các cơ quan, sở, ban, ngành, địa phương 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 lực lượng chuyên trách an ninh mạng tại địa phương. Thiết lập vận hành hiệu quả cơ chế phản ứng nhanh giữa lực lượng chuyên trách bảo vệ an ninh mạng, các đơn vị cung cấp dịch vụ viễn thông, nhà mạng, doanh nghiệp công nghệ, chuyên gia để xử lý, ứng cứu sự cố an ninh mạng một cách kịp thời, hiệu quả.

- Phối hợp xây dựng, hoàn thiện và đưa vào vận hành hệ thống tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an ninh mạng; tổ chức 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 toàn hệ thống chính trị tại địa phương.

- Rà soát, điều chỉnh quy hoạch 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 của các luồng dữ liệu quốc gia, kết nối quốc tế trong mọi tình huống, kể cả khi xảy ra thảm họa, chiến tranh.

- 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 đối với 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 kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số; 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

- 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; huy động sức mạnh tổng hợp của các doanh nghiệp công nghệ, viễn thông và các tầng lớp nhân dân. 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.

- Phối hợp triển khai nguồn lực xây dựng nền công nghiệp an ninh mạng tự chủ, tự cường; có cơ chế đầu tư cho phát triển hệ sinh thái an toàn thông tin, an ninh mạng, ưu tiên phát triển các sản phẩm "Make in Vietnam"; ưu tiên làm chủ và sản xuất nội địa, ưu tiên sử dụng sản phẩm, giải pháp nội địa; trong đó, chú trọng làm chủ công nghệ, sản xuất và sử dụng các sản phẩm cốt lõi, nền tảng bao gồm: Giải pháp tường lửa, phòng, chống mã độc, bảo vệ thiết bị đầu cuối, nền tảng điện

toán đám mây và hệ điều hành dùng riêng. Triển khai cơ chế, chính sách hỗ trợ, thu hút doanh nghiệp công nghệ, cộng đồng khởi nghiệp sáng tạo tham gia phát triển hệ sinh thái an ninh mạng. Phối hợp triển khai công tác đánh giá, kiểm định, chứng nhận hợp chuẩn, hợp quy; tạo điều kiện thuận lợi cho doanh nghiệp thương mại hóa sản phẩm, dịch vụ, hướng tới xuất khẩu và cạnh tranh quốc tế.

- Đẩy mạnh đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao. 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 tại địa phương có kết nối, hỗ trợ từ các chuyên gia trong và ngoài địa phương, sẵn sàng huy động nguồn lực xã hội tham gia ứng cứu sự cố, tình huống nguy hiểm về an ninh mạng. Phối hợp, triển khai hoàn thiện cơ chế, thực hiện chính sách thu hút, đãi ngộ chuyên gia giỏi, nhân tài tham gia phục vụ công tác bảo đảm an ninh mạng tại địa phương.

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

- Tăng cường và làm sâu sắc hơn quan hệ hợp tác song phương, đa phương trên lĩnh vực an ninh mạng, trọng tâm là chia sẻ thông tin tình báo, cảnh báo sớm; phối hợp quốc tế phòng, chống và ứng phó sự cố tấn công mạng; điều tra, truy tố tội phạm mạng xuyên quốc gia; bảo đảm độc lập, tự chủ, chủ quyền quốc gia trong quá trình hợp tác, tiếp thu kinh nghiệm, công nghệ và chuẩn mực quốc tế về an ninh mạng.

- Phối hợp triển khai hiệu quả, thực chất Công ước của Liên hợp quốc về chống tội phạm mạng năm 2025 *(Công ước Hà Nội)* theo hướng dẫn của các bộ, ngành Trung ương. Phối hợp tham gia xây dựng và triển khai các khuôn khổ pháp lý, chuẩn mực chung của quốc tế; tham gia góp ý, phối hợp nghiên cứu, ban hành Tuyên bố quốc gia của Việt Nam về việc áp dụng luật pháp quốc tế trên không gian mạng để khẳng định chủ quyền và trách nhiệm quốc gia. Tăng cường phối hợp, chia sẻ thông tin với lực lượng chức năng các nước; cử cán bộ đi đào tạo, huấn luyện chuyên sâu tại nước ngoài và tích cực tham gia các cuộc diễn tập an ninh mạng quốc tế *(nếu có)*.

III- TỔ CHỨC THỰC HIỆN

1. Các cơ quan tham mưu, giúp việc Tỉnh ủy, đảng trực thuộc Tỉnh ủy, Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh tổ chức quán triệt, xây dựng chương trình, kế hoạch thực hiện Chỉ thị số 57-CT/TW và Chương trình này; báo cáo kết quả cho Ban Thường vụ Tỉnh ủy *(qua Đảng ủy Công an tỉnh)* theo định kỳ hằng năm.

2. Đảng ủy Ủy ban nhân dân tỉnh lãnh đạo, chỉ đạo các cơ quan, đơn vị có liên quan kịp thời báo cáo, tham mưu, đề xuất các cấp, các ngành có liên quan trong xây dựng, ban hành cơ chế, chính sách đột phá đặc thù, ưu đãi vượt trội để thu hút, giữ chân các chuyên gia, nhân tài an ninh mạng, đào tạo nhân lực chất

lượng cao cho địa phương. Đồng thời, chỉ đạo làm tốt công tác an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng tại địa phương.

Lãnh đạo Ủy ban nhân dân tỉnh chỉ đạo Sở Giáo dục và Đào tạo chủ trì, phối hợp xây dựng chương trình, tổ chức đào tạo nguồn nhân lực an ninh mạng chất lượng cao; tích hợp kiến thức an ninh mạng vào hệ thống giáo dục quốc dân theo hướng dẫn, chỉ đạo của Bộ Giáo dục và Đào tạo phù hợp với tình hình thực tế tại địa phương.

3. Ban Tuyên giáo và Dân vận Tỉnh ủy chủ trì, phối hợp với các cơ quan liên quan tham mưu Ban Thường vụ Tỉnh ủy chỉ đạo, định hướng công tác tuyên truyền, phổ biến, quán triệt Chỉ thị số 57-CT/TW và Chương trình này sâu rộng trong toàn Đảng và toàn xã hội.

4. Đảng ủy Công an tỉnh chịu trách nhiệm thực hiện công tác quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu *(trừ lĩnh vực quân sự, cơ yếu)*; quản lý nhà nước về sản phẩm mật mã an ninh. Chủ trì, phối hợp triển khai Bộ chỉ số bảo đảm an ninh mạng quốc gia và tổ chức đánh giá, xếp hạng định kỳ hằng năm đối với các sở, ban, ngành, địa phương *(ngay sau khi Đảng ủy Công an Trung ương xây dựng, triển khai)*.

Phối hợp với các đơn vị nghiệp vụ thuộc Bộ Công an nghiên cứu, xây dựng, phát triển và ứng dụng sản phẩm mật mã dân sự vào công tác bảo đảm an ninh mạng quốc gia theo quy định; triển khai các nhiệm vụ về phát triển và ứng dụng sản phẩm mật mã an ninh; chỉ đạo huy động các nguồn lực xã hội tham gia bảo vệ an ninh mạng quốc gia. Đẩy mạnh kết nối, sử dụng dữ liệu từ cơ sở dữ liệu quốc gia về dân cư để thống nhất định danh không gian mạng toàn diện.

Phối hợp với các tổ chức, doanh nghiệp cung cấp dịch vụ viễn thông, Internet, dịch vụ tài chính ngân hàng trên địa bàn triển khai xử lý dứt điểm tình trạng SIM "rác", tài khoản "ảo" và thiết lập trật tự, kỷ cương trong quản lý người dùng mạng xã hội; 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.

5. Đảng ủy Quân sự tỉnh chủ trì, phối hợp với các cơ quan liên quan 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 của Bộ Quốc phòng. Tiếp tục tham mưu, triển khai hiệu quả Kế hoạch số 1164/KH-BQP, ngày 26/02/2026 của Bộ Quốc phòng về thực hiện Chỉ thị số 57-CT/TW.

6. Văn phòng Tỉnh ủy chủ trì tham mưu Ban Thường vụ Tỉnh ủy chỉ đạo triển khai các văn bản, quy định về công tác cơ yếu, quy định của Ban Cơ yếu Chính phủ trong quản lý nhà nước về mật mã *(bao gồm cả mật mã dân sự)*. Triển khai các loại sản phẩm mật mã cho các tổ chức, cá nhân trong hệ thống chính trị trên địa bàn tỉnh bảo đảm theo đúng quy định. Phối hợp chặt chẽ với Đảng ủy Công an tỉnh và các cơ

quan liên quan trong công tác bảo đảm an ninh, an toàn hệ thống mạng dữ liệu chuyên dùng và mạng internet trong các cơ quan, đơn vị trên địa bàn tỉnh.

7. Giao Đảng ủy Công an tỉnh chủ trì, phối hợp với Văn phòng Tỉnh ủy, Đảng ủy Ủy ban nhân dân tỉnh và các cơ quan liên quan theo dõi, đôn đốc, kiểm tra việc thực hiện Chỉ thị số 57-CT/TW và Chương trình này; định kỳ tham mưu Ban Thường vụ Tỉnh ủy báo cáo Ban Bí thư, Đảng ủy Công an Trung ương theo quy định. Đồng thời, tiếp tục phát huy vai trò Cơ quan Thường trực trong việc tham mưu cho Tiểu ban chỉ đạo An ninh mạng tỉnh chỉ đạo triển khai thực hiện tốt công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh.

T/M BAN THƯỜNG VỤ
PHÓ BÍ THƯ THƯỜNG TRỰC

ĐẢNG CỘNG SẢN VIỆT NAM
TỈNH ỦY LÂM ĐỒNG

Đặng Hồng Sỹ

Nơi nhận:
- Ban Bí thư Trung ương Đảng,
- Văn phòng Trung ương Đảng, (b/c)
- Đảng ủy Công an Trung ương,
- Các cơ quan tham mưu, giúp việc Tỉnh ủy,
- Đảng ủy trực thuộc tỉnh ủy,
- Đảng ủy các xã, phường, đặc khu,
- Các sở, ban, ngành của tỉnh,
- Các đồng chí Tỉnh ủy viên,
- Lưu Văn phòng Tỉnh ủy, NC2.