ỦY BAN NHÂN DÂN TỈNH NINH BÌNH	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 149 /KH-UBND	*Ninh Bình, ngày 05 tháng 5 năm 2026*

KẾ HOẠCH

Thực hiện Chương trình hành động số 24-CTr/TU, ngày 31/3/2026 của Ban Thường vụ Tỉnh ủy 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 trên địa bàn tỉnh

Thực hiện Chương trình hành động số 24-CTr/TU, ngày 31/3/2026 của Ban Thường vụ Tỉnh ủy 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 trên địa bàn tỉnh, Ủy ban nhân dân tỉnh ban hành Kế hoạch triển khai thực hiện, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Quán triệt thực hiện nghiêm túc quan điểm chỉ đạo của Ban Bí thư, của Tỉnh uỷ về tầm quan trọng đặc biệt của công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị và các mục tiêu, nhiệm vụ, giải pháp, chỉ tiêu đã được giao trong Chương trình hành động số 24-CTr/TU, ngày 31/3/2026 của Ban Thường vụ Tỉnh ủy.

2. Bảo đảm sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý tập trung, thống nhất của Nhà nước; phát huy sức mạnh tổng hợp của cả hệ thống chính trị và toàn dân, xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng; trong đó lực lượng Công an tỉnh, Quân sự tỉnh đóng vai trò nòng cốt.

3. Nâng cao hiệu lực, hiệu quả quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu; bảo đảm sự chỉ đạo, điều hành thông suốt, an toàn của các cơ quan trong hệ thống chính trị. Đưa công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ thường xuyên, trọng yếu, trách nhiệm của cả hệ thống chính trị và toàn dân; là nền tảng quan trọng để phát triển kinh tế số, xã hội số, chính quyền số và đô thị thông minh của tỉnh Ninh Bình, đồng thời góp phần giữ vững ổn định chính trị, bảo đảm quốc phòng - an ninh.

4. 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.

5. Việc triển khai thực hiện phải bảo đảm sự lãnh đạo thống nhất, đồng bộ từ tỉnh đến cơ sở; gắn trách nhiệm cụ thể của người đứng đầu cơ quan, đơn vị, địa phương.

II. CHỈ TIÊU

1. Chỉ tiêu tổng quát

Xây dựng không gian mạng trên địa bàn tỉnh an toàn, lành mạnh, tin cậy;

nâng cao năng lực tự chủ, tự cường về an ninh mạng; bảo vệ vững chắc an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng; bảo đảm an toàn hệ thống thông tin của các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội; bảo vệ dữ liệu cá nhân, dữ liệu quan trọng, bí mật nhà nước, phục vụ hiệu quả nhiệm vụ chuyển đổi số, phát triển kinh tế - xã hội, củng cố quốc phòng, an ninh của tỉnh.

2. Chỉ tiêu cụ thể

2.1. Chỉ tiêu đến năm 2026

- 100% cán bộ lãnh đạo, quản lý cấp tỉnh, cấp xã được tập huấn về an ninh mạng và bảo vệ dữ liệu.

- 100% hệ thống thông tin của các cơ quan Đảng, Nhà nước kết nối giám sát an ninh mạng tập trung của tỉnh.

2.2. Chỉ tiêu đến năm 2030

- Hình thành hệ sinh thái an ninh mạng cấp tỉnh, có sự tham gia của doanh nghiệp công nghệ số.

- Xây dựng đội ngũ chuyên gia an ninh mạng nòng cốt của tỉnh (50 - 100 người).

- 100% hệ thống thông tin quan trọng của tỉnh, hệ thống thông tin phục vụ sự lãnh đạo, chỉ đạo, điều hành của cấp ủy, chính quyền các cấp được rà soát, phân loại, kiểm tra, đánh giá an ninh mạng định kỳ (năm 2026 và duy trì các năm tiếp theo).

- 100% hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh được xác định, phê duyệt cấp độ an toàn thông tin (năm 2026 và duy trì các năm tiếp theo).

- 100% hồ sơ thiết kế hệ thống thông tin, dự án chuyển đổi số trên địa bàn tỉnh được thẩm định an ninh mạng, an ninh dữ liệu trước khi đầu tư xây dựng (năm 2026 và duy trì các năm tiếp theo).

- 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, kết nối, chia sẻ thông tin với các hệ thống giám sát an ninh mạng của Trung ương theo quy định (trước năm 2028).

- Hằng năm, tổ chức ít nhất 01 cuộc diễn tập an ninh mạng cấp tỉnh để nâng cao năng lực chỉ huy, điều hành, phối hợp và ứng phó, khắc phục sự cố an ninh mạng trong tình huống thực tế; trên 90% cán bộ, đảng viên được tuyên truyền, tập huấn, bồi dưỡng kiến thức, kỹ năng mới về an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

III. NHIỆM VỤ, GIẢI PHÁP CHỦ YẾU

1. Tăng cường công tác tuyên truyền, nâng cao nhận thức và trách nhiệm trong bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu

- Tổ chức quán triệt, triển khai nghiêm túc Chỉ thị số 57-CT/TW và Chương trình hành động số 24-CTr/TU, ngày 31/3/2026 của Ban Thường vụ Tỉnh ủy đến

toàn thể cán bộ, đảng viên, công chức, viên chức và người lao động trong hệ thống chính trị.

- Nâng cao nhận thức của người đứng đầu cơ quan, đơn vị về vai trò, tầm quan trọng của công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; xác định đây là nhiệm vụ thường xuyên, trọng yếu, gắn trực tiếp với trách nhiệm lãnh đạo, quản lý. Kết quả công tác này là một trong những tiêu chí quan trọng để đánh giá mức độ hoàn thành nhiệm vụ của người đứng đầu.

- Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, phổ biến, giáo dục kiến thức, kỹ năng an ninh mạng; phòng, chống tội phạm mạng cho các tầng lớp nhân dân, nhất là thế hệ trẻ; tăng cường tuyên truyền về an ninh mạng trong trường học; phát huy hiệu quả phong trào "Bình dân học vụ số" để xây dựng "thế hệ công dân số" văn minh, tuân thủ pháp luật.

- Tổ chức các chương trình đào tạo, tập huấn, bồi dưỡng kiến thức, kỹ năng về an ninh mạng, an toàn dữ liệu cho cán bộ, công chức, viên chức; chú trọng đào tạo chuyên sâu cho lực lượng chuyên trách.

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

- Khẩn trương rà soát sửa đổi, bổ sung, hoàn thiện các quy định của 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.

- Nghiên cứu ban hành Quy chế bảo đảm an ninh mạng trong các cơ quan Đảng, Nhà nước của tỉnh; Quy chế chia sẻ dữ liệu giữa các cơ quan trong hệ thống chính trị của tỉnh; Quy định về bảo vệ dữ liệu cá nhân trong hệ thống thông tin của tỉnh.

- Duy trì hiệu quả hoạt động Tiểu ban An ninh mạng tỉnh, thành lập Văn phòng Tiểu ban để tham mưu, giúp việc cho Tiểu ban.

- Thực hiện hiệu quả Quy chế của UBND tỉnh về phối hợp theo dõi, xử lý thông tin xấu độc trên không gian mạng.

- Tổ chức rà soát, thống kê, phân loại toàn bộ hệ thống thông tin trên địa bàn tỉnh; thực hiện nghiêm việc xác định, thẩm định, phê duyệt cấp độ an toàn thông tin theo quy định.

- Áp dụng phương thức quản trị rủi ro trong bảo đảm an ninh mạng; chuyển từ quản lý kỹ thuật sang quản lý tổng thể, chủ động phòng ngừa.

- Triển khai các giải pháp xác thực danh tính người dùng trên không gian mạng theo quy định.

- Xây dựng và triển khai cơ chế phối hợp giữa các cơ quan nhà nước với doanh nghiệp viễn thông, Internet, tài chính - ngân hàng trong bảo đảm an ninh mạng và phòng, chống tội phạm công nghệ cao.

- Tăng cường công tác thanh tra, kiểm tra, giám sát việc chấp hành pháp luật về an ninh mạng, bảo vệ dữ liệu; công tác điều tra, xử lý tội phạm sử dụng

công nghệ cao; bảo vệ quyền, lợi ích hợp pháp của tổ chức, cá nhân.

- Phối hợp với các doanh nghiệp viễn thông, Internet: rà soát, xử lý SIM rác, tài khoản ảo; kiểm soát thông tin xấu độc trên không gian mạng.

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

- Tập trung đầu tư xây dựng, đưa vào vận hành Trung tâm An ninh mạng của tỉnh, bảo đảm chức năng giám sát, cảnh báo sớm, phát hiện và xử lý sự cố an ninh mạng. Triển khai xây dựng hệ thống phòng, chống mã độc quản trị tập trung trên địa bàn tỉnh.

- Rà soát, quy hoạch lại hạ tầng công nghệ thông tin theo hướng tập trung, đồng bộ; chuyển các hệ thống về trung tâm dữ liệu đạt tiêu chuẩn an toàn.

- Kiên quyết loại bỏ, thay thế các hệ thống thông tin không bảo đảm yêu cầu an toàn, an ninh mạng.

- Tăng cường bảo vệ các hệ thống thông tin và cơ sở dữ liệu trọng yếu của tỉnh (dân cư, đất đai, y tế, tài chính, du lịch...).

- Áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin; tổ chức kiểm tra, đánh giá định kỳ, phát hiện và khắc phục kịp thời các lỗ hổng bảo mật.

- 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 tỉnh; huy động vai trò tham gia tích cực của các doanh nghiệp công nghệ, viễn thông và các tầng lớp nhân dân trong bảo đảm an ninh mạng, an ninh dữ liệu trên địa bàn.

- Phát động rộng rãi Phong trào toàn dân bảo vệ an ninh mạng; 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, phản bác với các thông tin xấu độc, sai sự thật trên không gian mạng.

- Xây dựng, phát triển đội ngũ cán bộ chuyên trách, bán chuyên trách về an ninh mạng tại các cơ quan, đơn vị.

- Tổ chức đào tạo, bồi dưỡng thường xuyên; kết hợp đào tạo cơ bản với đào tạo chuyên sâu, thực hành, diễn tập.

- Từng bước hình thành cụm doanh nghiệp công nghệ số của tỉnh, tập trung vào các lĩnh vực: An ninh mạng, an toàn thông tin; phân tích, xử lý dữ liệu lớn (Big Data); điện toán đám mây, trí tuệ nhân tạo phục vụ quản lý, điều hành nhằm tạo hệ

sinh thái công nghệ phục vụ chuyển đổi số và bảo đảm an ninh mạng.

- Thành lập Tổ chuyên gia an ninh mạng của tỉnh với thành phần nòng cốt là lực lượng Công an, Quân đội, phối hợp với cán bộ kỹ thuật của các sở, ban, ngành liên quan để tham mưu, hỗ trợ kỹ thuật, ứng cứu sự cố.

- Tăng cường liên kết giữa cơ quan nhà nước - cơ sở đào tạo - doanh nghiệp trong đào tạo, phát triển nguồn nhân lực. Xây dựng cơ chế, chính sách thu hút chuyên gia, nhân lực chất lượng cao trong lĩnh vực an ninh mạng làm việc tại tỉnh.

- Khuyến khích doanh nghiệp công nghệ số tham gia phát triển sản phẩm, dịch vụ an ninh mạng "Make in Vietnam".

5. Đẩy mạnh hợp tác quốc tế, phối hợp trong và ngoài tỉnh

- Tăng cường phối hợp với các bộ, ngành Trung ương trong triển khai các chương trình, dự án về an ninh mạng.

- Đẩy mạnh liên kết, hợp tác với các tỉnh, thành phố trong chia sẻ kinh nghiệm, hỗ trợ kỹ thuật.

- Mở rộng hợp tác với các doanh nghiệp công nghệ lớn trong triển khai các giải pháp an ninh mạng.

- Tham gia các chương trình, hoạt động hợp tác quốc tế về an ninh mạng theo quy định. Triển khai thực hiện hiệu quả, thực chất các nội dung của Công ước của Liên hợp quốc về chống tội phạm mạng năm 2025 (Công ước Hà Nội).

6. Tăng cường kiểm tra, giám sát và đánh giá

- Tổ chức kiểm tra, giám sát định kỳ và đột xuất việc triển khai thực hiện Kế hoạch tại các cơ quan, đơn vị.

- Thực hiện đánh giá hằng năm mức độ an toàn thông tin đối với các hệ thống thông tin trên địa bàn tỉnh.

- Áp dụng Bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng để xếp hạng các sở, ban, ngành, địa phương.

- Công khai kết quả đánh giá để nâng cao trách nhiệm, tạo động lực thi đua.

- Gắn kết quả thực hiện với công tác thi đua, khen thưởng và đánh giá mức độ hoàn thành nhiệm vụ của người đứng đầu.

IV. PHÂN CÔNG NHIỆM VỤ

Chi tiết tại Phụ Lục kèm theo.

V. KINH PHÍ THỰC HIỆN

1. Kinh phí thực hiện Kế hoạch: Từ nguồn ngân sách nhà nước và các nguồn hợp pháp khác.

2. Các sở, ngành, UBND các xã, phường nghiên cứu, chú trọng huy động vốn cho bảo vệ an ninh mạng dưới hình thức hợp tác công tư (PPP), tài trợ, viện trợ, đóng góp của doanh nghiệp, tổ chức cá nhân theo quy định của pháp luật.

VI. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành; UBND các xã, phường xây dựng kế hoạch cụ thể để triển khai thực hiện, hoàn thành trước ngày 20/5/2026; định kỳ báo cáo kết quả thực hiện về Công an tỉnh để tổng hợp, báo cáo UBND tỉnh. Thường xuyên rà soát, cập nhật, bổ sung các nhiệm vụ vào kế hoạch, chương trình công tác hằng năm của cơ quan, đơn vị mình để tổ chức triển khai thực hiện. Kết quả thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu là một trong các tiêu chí đánh giá mức độ hoàn thành nhiệm vụ, bình xét thi đua, khen thưởng hằng năm của người đứng đầu cơ quan, đơn vị.

2. Thủ trưởng các sở, ban, ngành; Chủ tịch UBND xã, phường: Chỉ đạo thực hiện nội dung nhiệm vụ, giải pháp cụ thể được giao tại Kế hoạch và Phụ lục kèm theo; tăng cường kiểm tra đôn đốc việc triển khai thực hiện; định kỳ 6 tháng (trước ngày 10/6) và hằng năm (trước ngày 30/11) tổng hợp kết quả thực hiện, báo cáo UBND tỉnh (qua Công an tỉnh).

3. Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ thường xuyên theo dõi, đôn đốc, hướng dẫn các cơ quan, đơn vị, địa phương triển khai thực hiện Kế hoạch; định kỳ 6 tháng (trước ngày 15/6) và hằng năm (trước ngày 10/12) hoặc đột xuất khi có yêu cầu, tổng hợp kết quả thực hiện, đề xuất những kiến nghị, giải pháp (nếu có), báo cáo UBND tỉnh theo quy định.

4. Sở Tài chính căn cứ vào tình hình thực tế và khả năng cân đối của ngân sách địa phương, phối hợp với các đơn vị liên quan tham mưu UBND tỉnh bố trí kinh phí thực hiện Kế hoạch theo phân cấp ngân sách nhà nước và các quy định hiện hành.

5. Trong quá trình tổ chức thực hiện, nếu thấy cần sửa đổi, bổ sung, các cơ quan, đơn vị chủ động đề xuất, trao đổi Công an tỉnh để tổng hợp, báo cáo UBND tỉnh xem xét, quyết định./.

Nơi nhận:
- Thường trực Tỉnh ủy;
- CT các PCT UBND tỉnh;
- Các sở, ban, ngành, đoàn thể;
- Công an tỉnh;
- Bộ Chỉ huy quân sự tỉnh;
- UBND các xã, phường;
- Báo và PTTH NB;
- Văn phòng Đảng ủy UBND tỉnh;
- Trung tâm Thông tin - Công báo;
- Lưu: VT, VP11.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Đặng Thanh Sơn