ỦY BAN NHÂN DÂN TỈNH HÀ TĨNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 197 /KH-UBND	*Hà Tĩnh, ngày 15 tháng 4 năm 2026*

KẾ HOẠCH
Bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị

Thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2026 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, Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị, Chương trình hành động số 10-CTr/TU ngày 12/02/2026 của Ban Thường vụ Tỉnh ủy về thực hiện Chỉ thị số 57-CT/TW; xét đề nghị của Công an tỉnh tại văn bản số 670/CAT-ANM ngày 25/02/2026 và văn bản số 1075/CAT-ANM ngày 26/3/2026; trên cơ sở ý kiến thống nhất của các thành viên Ủy ban nhân dân tỉnh tại cuộc họp ngày 25/3/2026 (Thông báo số 140/TB-UBND ngày 25/3/2026), Ủy ban nhân dân tỉnh ban hành Kế hoạch triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục tiêu chung

Xây dựng không gian mạng trên địa bàn tỉnh an toàn, vững mạnh, có năng lực phòng vệ tốt và khả năng chống chịu cao, góp phần bảo vệ vững chắc chủ quyền, an ninh và lợi ích của quốc gia trên không gian mạng.

2. Mục tiêu cụ thể

2.1. Trong năm 2026

- **Về công tác lãnh đạo, chỉ đạo:** tạo chuyển biến mạnh mẽ về nhận thức và hành động trong toàn hệ thống chính trị và xã hội.

- **Về thể chế:** ban hành các văn bản, hướng dẫn triển khai thực hiện các văn bản quy phạm pháp luật về cơ chế pháp lý để khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp mới tham gia thị trường trên địa bàn tỉnh, gỡ bỏ các rào cản thủ tục hành chính.

- **Về hạ tầng:** xây dựng và phát triển hạ tầng an ninh mạng trên địa bàn tỉnh hiện đại, đồng bộ, đủ năng lực bảo vệ chủ quyền không gian mạng: (1) các hệ thống thông tin của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội được rà soát, khắc phục các lỗ hổng, điểm yếu bảo mật về an ninh mạng; (2) các hệ thống thông tin quan trọng thuộc danh mục được ưu tiên bảo vệ của hệ thống chính trị từ cấp độ 3 trở lên *(trừ hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu)* được kết nối, chia sẻ thông tin, dữ liệu giám sát an ninh mạng 24/7 với Trung tâm An ninh mạng tỉnh và Trung tâm An ninh

mạng quốc gia (Bộ Công an); [3] xây dựng và ban hành các tiêu chuẩn, quy chuẩn kỹ thuật cho sản phẩm, dịch vụ an ninh mạng; [4] bảo đảm hạ tầng mật mã hoạt động ổn định, bảo mật phục vụ trao đổi dữ liệu bí mật nhà nước xuyên suốt từ Trung ương đến 100% xã, phường trên địa bàn tỉnh.

- **Nhân lực:** nâng cao nhận thức của cán bộ, đảng viên và người dân về bảo mật thông tin, an ninh mạng và an ninh dữ liệu. Tăng cường đào tạo, bồi dưỡng đội ngũ cán bộ, chuyên gia an ninh mạng chất lượng cao tại các sở, ban, ngành, địa phương, cơ quan, doanh nghiệp trên địa bàn tỉnh.

- **Quản trị:** tăng cường kỷ luật, kỷ cương trong quản lý nhà nước về an ninh mạng. Thực hiện quản trị an ninh mạng dựa trên đánh giá rủi ro, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật.

- **Công nghệ:** thúc đẩy ứng dụng các công nghệ tiên tiến như trí tuệ nhân tạo, phân tích dữ liệu lớn, giám sát thông minh để phát hiện sớm và xử lý kịp thời các mối đe dọa và các nguy cơ về an ninh mạng. Chuyển đổi sang mô hình phòng thủ chủ động, ứng dụng các giải pháp mã hoá hiện đại phục vụ bảo vệ dữ liệu quan trọng, dữ liệu bí mật và giao dịch của Nhà nước. Khuyến khích nghiên cứu, phát triển và làm chủ các công nghệ an ninh mạng thế hệ mới, tăng cường năng lực tự chủ công nghệ, tham gia tích cực vào hệ sinh thái công nghiệp an ninh mạng quốc gia vững mạnh.

2.2. Đến năm 2030

- **Chỉ số an toàn, an ninh mạng:** tiếp tục triển khai các giải pháp nâng cao Chỉ số an toàn, an ninh mạng góp phần đưa Việt Nam tiếp tục duy trì xếp hạng 20 quốc gia có mức đánh giá cao về Chỉ số an toàn, an ninh mạng toàn cầu (GCI) của Liên minh Viễn thông Quốc tế (ITU).

- **Thể chế**: tiếp tục ban hành các văn bản, hướng dẫn để khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp mới tham gia thị trường sản phẩm, giải pháp an ninh mạng chất lượng có cơ hội phát triển. Triển khai đầy đủ các văn bản quy định của pháp luật để răn đe và phản ứng nhanh với các hành vi vi phạm pháp luật trên không gian mạng trên địa bàn tỉnh.

- **Hạ tầng:** xây dựng và đưa vào vận hành hiệu quả kiến trúc bảo vệ an ninh mạng đa lớp hiện đại, đồng bộ, hiệu quả, góp phần bảo đảm chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu. Ban hành quy hoạch hạ tầng công nghệ thông tin tổng thể của tỉnh theo chỉ đạo, định hướng của Trung ương.

- **Nhân lực:** đào tạo, bồi dưỡng, xây dựng đội ngũ chuyên gia an ninh mạng có trình độ cao, trước mắt đáp ứng nhu cầu trên địa bàn tỉnh và hướng đến cung cấp nguồn nhân lực cho các tổ chức, doanh nghiệp trong và ngoài nước.

- **Quản trị:** các sở, ban, ngành, đơn vị, địa phương và các tổ chức vận hành hạ tầng thông tin quan trọng trên địa bàn phải triển khai và áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia.

- **Công nghệ:** ưu tiên sử dụng các sản phẩm, dịch vụ an ninh mạng "Make in Vietnam", phấn đấu chiếm trên 50% thị trường trong tỉnh. Nghiên cứu đề xuất

Trung ương xây dựng các trung tâm nghiên cứu, sản xuất các sản phẩm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trên địa bàn.

2.3. Tầm nhìn chiến lược đến năm 2045

Bảo đảm vững chắc an ninh mạng trên địa bàn tỉnh góp phần đưa nền an ninh mạng quốc gia bền vững, tự chủ, có năng lực cạnh tranh toàn cầu. Phát triển hạ tầng an ninh mạng và hạ tầng số trên địa bàn tỉnh hiện đại. Thu hút đầu tư, xây dựng các trung tâm đổi mới sáng tạo, khu công nghiệp công nghệ cao, các doanh nghiệp về ngành công nghiệp an ninh mạng trên địa bàn tỉnh.

3. Yêu cầu

- Kế hoạch phải được quán triệt và triển khai thống nhất trong toàn bộ hệ thống chính trị, tránh dàn trải, cục bộ, thiếu tập trung.

- Nhiệm vụ phải được tổ chức thực hiện với quyết tâm cao, có sản phẩm cụ thể, đo lường được, bảo đảm tiến độ và hiệu quả thực chất.

- Phát huy tối đa tiềm năng, trí tuệ, gắn với tiếp thu, làm chủ và ứng dụng hiệu quả các thành tựu công nghệ, kỹ thuật tiên tiến trong và ngoài nước.

- Gắn trách nhiệm người đứng đầu với kết quả bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu, coi đây là tiêu chí quan trọng trong đánh giá, quy hoạch, bổ nhiệm cán bộ lãnh đạo, quản lý các cấp.

II. NHIỆM VỤ TRỌNG TÂM NĂM 2026

1. Tham mưu Tỉnh ủy kiện toàn Tiểu ban An ninh mạng tỉnh do đồng chí Bí thư Tỉnh ủy làm Trưởng Tiểu ban, chỉ đạo toàn diện, xuyên suốt công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh.

2. Các cơ quan được giao quản lý, vận hành, phụ trách các cơ sở dữ liệu, hệ thống thông tin trên địa bàn tỉnh có trách nhiệm: (1) rà soát, khắc phục tổng thể về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với hệ thống thông tin theo tiêu chuẩn TCVN 14423:2025 và nguồn nhân lực thuộc phạm vi quản lý; (2) triển khai giám sát an ninh mạng tại cơ quan, đơn vị thuộc phạm vi quản lý; (3) báo cáo định kỳ và đột xuất kết quả, tiến độ, mức độ tuân thủ về cơ quan có thẩm quyền và kiến nghị biện pháp hoàn thiện thể chế, tiêu chuẩn, phân bổ nguồn lực khi cần thiết; (4) xác định trách nhiệm của người đứng đầu về an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

3. Nâng cấp Trung tâm An ninh mạng tỉnh, bảo đảm 100% hệ thống thông tin quan trọng trong hệ thống chính trị trên địa bàn tỉnh *(hệ thống thông tin cấp độ 3 trở lên, trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu)* được giám sát, cảnh báo an ninh mạng 24/7 và kết nối, chia sẻ dữ liệu đến Trung tâm An ninh mạng quốc gia.

4. Rà soát, đánh giá công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với các hệ thống thông tin của các cơ quan, đơn vị, địa phương, doanh nghiệp trên địa bàn tỉnh từ khâu thiết kế, tạo lập đến triển khai, vận hành. Tổ chức và hướng dẫn diễn tập, thực hành xử lý các tình huống về an ninh mạng,

an toàn thông tin đối với các hệ thống thông tin trên địa bàn tỉnh, nâng cao khả năng phối hợp ứng phó, phối hợp xử lý nhanh, hiệu quả giữa các lực lượng khi xảy ra sự cố, với lực lượng nòng cốt là Đội ứng cứu sự cố an ninh mạng tỉnh. Các hệ thống thông tin quan trọng, trước khi đưa vào vận hành, sử dụng bắt buộc thực hiện kiểm thử xâm nhập để kịp thời phát hiện, khắc phục lỗ hổng bảo mật.

5. Ban hành các quy định, tài liệu hướng dẫn về kiểm tra, đánh giá, bảo đảm an ninh mạng, an toàn thông tin cho các cơ sở dữ liệu, hệ thống dùng chung trên địa bàn. Định kỳ tổ chức kiểm tra, đánh giá và hướng dẫn việc thực hiện các quy định bảo đảm an ninh mạng, an toàn thông tin.

6. Triển khai hiệu quả cơ chế ưu đãi đặc biệt và chính sách ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng, bảo mật thông tin và an ninh dữ liệu "Make in Vietnam".

7. Rà soát, trình cấp có thẩm quyền xem xét ban hành hoặc điều chỉnh quy hoạch hạ tầng công nghệ thông tin tổng thể của tỉnh theo hướng tập trung, chuẩn hóa trung tâm dữ liệu theo hướng dẫn, chỉ đạo của Trung ương. Đầu tư, nâng cấp hạ tầng công nghệ thông tin đáp ứng yêu cầu và tuân thủ quy hoạch được ban hành.

III. NHIỆM VỤ ĐẾN NĂM 2030

1. Nâng cao nhận thức cho toàn hệ thống chính trị và người dân

- Triển khai các chương trình đào tạo, bồi dưỡng, phổ biến kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số".

- Đẩy mạnh truyền thông đại chúng và trên mạng xã hội cho người dân kỹ năng nhận diện, phòng, chống lừa đảo, tiếp nhận và xử lý phản ánh sự cố.

- Đưa các nội dung kiến thức, kỹ năng cơ bản về 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 theo hướng dẫn của Trung ương.

- Triển khai các giải pháp định danh và đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng, củng cố lòng tin, trách nhiệm của người dân khi tham gia hoạt động, tương tác, làm việc trên không gian mạng.

- Đưa tiêu chí bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu vào đánh giá xếp loại thi đua, khen thưởng đối với các cơ quan, đơn vị, địa phương trên địa bàn tỉnh.

2. Xây dựng và hoàn thiện thể chế, khung pháp lý

- Tiếp tục rà soát, sửa đổi, bổ sung, điều chỉnh các văn bản chỉ đạo, hướng dẫn về lĩnh vực an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

- Áp dụng đúng các tiêu chuẩn quốc gia và quy chuẩn kỹ thuật đối với hạ tầng công nghệ thông tin tại các cơ quan, đơn vị, địa phương trên địa bàn, tập trung vào các hệ thống ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự an toàn xã hội và đời sống Nhân dân.

- Triển khai Khung quản trị rủi ro an ninh mạng quốc gia và chỉ số đánh giá năng lực bảo đảm an ninh mạng theo hướng dẫn.

- Tích cực trao đổi, chia sẻ thông tin về an ninh mạng trong nước và quốc tế theo cơ chế được hướng dẫn.

3. Phát triển hạ tầng an ninh mạng hiện đại, đồng bộ, đáp ứng yêu cầu bảo vệ chủ quyền quốc gia trên không gian mạng

- Triển khai kiến trúc bảo vệ an ninh mạng quốc gia đa lớp hỗ trợ bảo vệ cho toàn bộ hạ tầng mạng Internet và các hệ thống thông tin của các đơn vị, địa phương, doanh nghiệp trên địa bàn.

- Quy hoạch và triển khai đồng bộ các nhóm giải pháp: (1) bảo vệ hạ tầng mạng; (2) bảo vệ thiết bị đầu cuối; (3) bảo vệ ứng dụng, dịch vụ; (4) bảo vệ dữ liệu; (5) bảo vệ người dùng.

- Tập trung nguồn lực hỗ trợ các đơn vị, doanh nghiệp trên địa bàn tỉnh nghiên cứu, 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 nghiên cứu, phát triển và ứng dụng mật mã dân sự phục vụ bảo mật thông tin.

- Bảo vệ tuyệt đối an toàn các hệ thống thông tin quan trọng, các cơ sở dữ liệu quốc gia về dân cư, đất đai, tài chính, y tế, giáo dục, bảo hiểm, tư pháp… Triển khai cơ chế thống nhất về tiêu chuẩn, quy chuẩn bảo mật, bảo đảm an ninh mạng "ngay từ thiết kế" đối với các trung tâm dữ liệu trong tỉnh, các hệ thống số, nền tảng số và ứng dụng mới. Rà soát, phát hiện và khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin. Kết nối, chia sẻ dữ liệu liên thông giữa địa phương với các ban, bộ, ngành Trung ương trên nguyên tắc bảo mật, an toàn, tuân thủ đúng quy định của pháp luật.

4. Phát triển công nghiệp an ninh mạng tự chủ và thị trường an ninh mạng cạnh tranh, minh bạch

- Hỗ trợ tích cực cho phát triển hệ sinh thái an ninh mạng, đặc biệt là hệ sinh thái "*Make in Vietnam*".

- Xây dựng thị trường cạnh tranh lành mạnh, minh bạch. Hình thành các trung tâm nghiên cứu, vườn ươm hỗ trợ khởi nghiệp và không gian đổi mới sáng tạo để hỗ trợ doanh nghiệp, nhất là các doanh nghiệp khởi nghiệp sáng tạo nhằm thúc đẩy gắn kết giữa nghiên cứu - triển khai - thương mại hóa sản phẩm.

- Ưu tiên sử dụng các sản phẩm, giải pháp nội địa đáp ứng được các tiêu chuẩn, quy chuẩn trong các dự án, hệ thống trọng yếu nhằm vừa tạo thị trường, vừa thúc đẩy và hỗ trợ doanh nghiệp Việt Nam phát triển, phù hợp chủ trương nâng cao khả năng tự chủ chiến lược của đất nước.

- Triển khai hiệu quả các tiêu chuẩn, quy chuẩn kỹ thuật về mã dân sự để bảo vệ an ninh mạng.

5. Bảo đảm nguồn lực tài chính, ngân sách

Quy định an ninh mạng, bảo mật thông tin, an ninh dữ liệu là thành phần bắt buộc trong mọi dự án công nghệ thông tin, bảo đảm ưu tiên tối đa nguồn lực chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu

trong triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí.

6. Bảo đảm nguồn nhân lực

- Đẩy mạnh đào tạo, bồi dưỡng, phát triển nguồn nhân lực an ninh mạng cả về số lượng và chất lượng, trong đó chú trọng nâng cao nhận thức chiến lược và năng lực chỉ đạo của lãnh đạo, quản lý và đào tạo chuyên sâu, chuyên gia đầu ngành, xây dựng mạng lưới chuyên gia an ninh mạng trong và ngoài tỉnh tham gia tư vấn chính sách, hỗ trợ kỹ thuật, ứng cứu sự cố, xử lý các tình huống phức tạp, nhạy cảm về an ninh mạng.

- Tăng cường bố trí nhân lực bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các sở, ngành, địa phương, ưu tiên các cơ quan, đơn vị vận hành các hệ thống thông tin, cơ sở dữ liệu quan trọng của tỉnh. Triển khai cơ chế, chính sách thu hút, đãi ngộ chuyên gia phục vụ công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trên địa bàn tỉnh.

7. Hợp tác quốc tế trên lĩnh vực an ninh mạng

Tích cực hợp tác quốc tế trong lĩnh vực an ninh mạng, tăng cường trao đổi thông tin, kinh nghiệm trong điều tra số, phòng, chống tội phạm sử dụng công nghệ cao, ứng phó sự cố tấn công mạng. Tham gia triển khai thực hiện hiệu quả, thực chất Công ước của Liên hợp quốc về chống tội phạm mạng năm 2025 phù hợp với tình hình và điều kiện thực tế của tỉnh.

IV. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

- Chủ trì triển khai công tác quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với toàn bộ các cơ quan thuộc hệ thống chính trị trên địa bàn tỉnh (*trừ lĩnh vực quân sự, quốc phòng và cơ yếu*). Giữ vai trò thường trực về vấn đề an ninh mạng, bảo mật thông tin và an ninh dữ liệu (*nhiệm vụ thực hiện thường xuyên*).

- Nâng cấp, mở rộng và nâng cao năng lực giám sát của Trung tâm An ninh mạng tỉnh, bảo đảm 100% các hệ thống thông tin, cơ sở dữ liệu quan trọng, dùng chung của tỉnh được giám sát, cảnh báo an ninh mạng 24/7 và thực hiện kết nối, chia sẻ dữ liệu giám sát, cảnh báo đến Trung tâm An ninh mạng quốc gia (*hoàn thành giai đoạn 2 trong tháng 11/2026*). Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan điều phối, ứng phó các sự cố về an ninh mạng trên địa bàn tỉnh (*nhiệm vụ thực hiện thường xuyên*).

- Chủ trì, phối hợp với Sở Giáo dục và Đào tạo, Báo và Phát thanh, truyền hình Hà Tĩnh tổ chức các chiến dịch truyền thông sâu rộng trên truyền hình, báo chí, mạng xã hội, kết hợp cảnh báo trực tiếp qua các nhà mạng, ngân hàng, nền tảng số. Tổ chức phổ cập kỹ năng an toàn số cho người dân thông qua các chương trình giáo dục, tập huấn cộng đồng và tài liệu hướng dẫn trực tuyến. Phối hợp triển khai hệ thống tiếp nhận, xử lý phản ánh 24/7 liên thông giữa cơ quan chức năng, tổ chức doanh nghiệp và người dân nhằm ngăn chặn kịp thời các hình thức lừa đảo trực tuyến (*nhiệm vụ thực hiện thường xuyên*).

- Phối hợp với Sở Khoa học và Công nghệ và các đơn vị có liên quan hằng năm đánh giá năng lực bảo đảm an ninh mạng của các cơ quan, đơn vị, địa phương, doanh nghiệp trên địa bàn tỉnh; tổ chức xếp hạng các đơn vị, địa phương trong phát triển khoa học, công nghệ, chuyển đổi số (*nhiệm vụ thực hiện thường xuyên*).

- Chủ trì đánh giá, thẩm định công tác an ninh mạng, bảo mật thông tin, an ninh dữ liệu là thành phần bắt buộc trong mọi dự án công nghệ thông tin. Đánh giá kinh phí chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí (*nhiệm vụ thực hiện thường xuyên*).

- Tổ chức hậu kiểm và đánh giá hiệu quả việc thực hiện ngân sách cho an ninh mạng, trong đó ưu tiên sử dụng cho các sản phẩm "Make in Vietnam" đã qua kiểm định, đánh giá chất lượng (*nhiệm vụ thực hiện thường xuyên*).

- Phối hợp với Sở Giáo dục và Đào tạo và các đơn vị có liên quan tổ chức: (1) các khóa đào tạo, bồi dưỡng, cập nhật kiến thức, kỹ năng thực tế về công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho cán bộ chuyên trách an ninh mạng tại các đơn vị, địa phương; (2) triển khai phổ biến kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số" cho người sử dụng mạng *(nhiệm vụ thực hiện thường xuyên).*

- Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng, củng cố lòng tin, trách nhiệm của người dân khi tham gia hoạt động, tương tác, làm việc trên không gian mạng. Triển khai hiệu quả, có thực chất Công ước Hà Nội về chống tội phạm mạng năm 2025 (*nhiệm vụ thực hiện thường xuyên*).

2. Bộ Chỉ huy Quân sự tỉnh

- Triển khai công tác bảo đảm an ninh mạng, mật mã, bảo mật thông tin và an ninh dữ liệu trong lĩnh vực quân sự, quốc phòng, cơ yếu thuộc phạm vi quản lý và theo chức năng, nhiệm vụ được giao. Phối hợp chặt chẽ, đồng bộ với các đơn vị có liên quan trong ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Hà Tĩnh (*nhiệm vụ thực hiện thường xuyên*).

- Thực hiện nhiệm vụ bảo đảm hạ tầng mật mã quốc gia hoạt động ổn định, an toàn phục vụ bảo mật, trao đổi bí mật nhà nước từ Trung ương đến 100% đơn vị cấp xã trên địa bàn tỉnh (*nhiệm vụ thực hiện thường xuyên*).

3. Sở Khoa học và Công nghệ

- Chủ trì, phối hợp với Công an tỉnh và các đơn vị liên quan triển khai phương án quy hoạch hạ tầng thông tin theo hướng tập trung máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện để triển khai đầy đủ các biện pháp bảo vệ an ninh mạng theo hướng dẫn của Bộ Khoa học và Công nghệ.

- Chủ trì, phối hợp với các đơn vị liên quan tham mưu triển khai các cơ chế, chính sách đặc thù thu hút, hỗ trợ các doanh nghiệp công nghệ trong nước hoạt động trên địa bàn tỉnh và ưu tiên sử dụng các sản phẩm, giải pháp, dịch vụ

an ninh mạng, bảo mật thông tin, an ninh dữ liệu "Make in Vietnam" theo hướng dẫn của Trung ương (*hoàn thành trong tháng 6/2026*).

- Phối hợp với Công an tỉnh, Sở Tài chính và các đơn vị có liên quan rà soát, tham mưu Ủy ban nhân dân tỉnh bố trí kinh phí bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các đơn vị, địa phương theo hướng tập trung, đồng bộ theo hướng dẫn của Trung ương (*nhiệm vụ thực hiện thường xuyên*).

4. Sở Giáo dục và Đào tạo

Chủ trì, phối hợp với Công an tỉnh và các đơn vị có liên quan tham mưu triển khai các nội dung:

- Tổ chức các khóa đào tạo thực tế về công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho cán bộ chuyên trách an ninh mạng tại các đơn vị, địa phương theo kế hoạch của Bộ, tỉnh (*nhiệm vụ thực hiện thường xuyên*).

- Tổ chức các chương trình đào tạo, tập huấn, bồi dưỡng kiến thức, kỹ năng sư phạm về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trên nền tảng "Bình dân học vụ số" theo kế hoạch của Bộ, tỉnh (*nhiệm vụ thực hiện thường xuyên*).

- Triển khai "Khung năng lực số và an toàn mạng toàn diện" trong chương trình giáo dục phổ thông trên địa bàn tỉnh, tích hợp các kỹ năng thực hành như nhận diện lừa đảo, quản lý danh tính số, ứng phó với bắt nạt trên mạng… vào các môn học chính khoá, giúp hình thành văn hoá số an toàn từ sớm cho thế hệ trẻ (*nhiệm vụ thực hiện thường xuyên*).

5. Sở Tài chính

- Tham mưu cấp có thẩm quyền phương án kinh phí thực hiện công tác bảo đảm an toàn, an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo phân cấp quản lý, phù hợp với khả năng cân đối ngân sách (*nhiệm vụ thực hiện thường xuyên*).

- Chủ trì hướng dẫn thực hiện các quy định về tài chính, công sản, ngân sách, đấu thầu có liên quan để tạo thuận lợi cho quá trình triển khai thực hiện, đáp ứng yêu cầu nhiệm vụ và đặc thù vòng đời ngắn của các sản phẩm, giải pháp bảo đảm an ninh mạng (*nhiệm vụ thực hiện thường xuyên*).

6. Đề nghị Báo và Phát thanh, truyền hình Hà Tĩnh

Chủ trì, phối hợp với các đơn vị có liên quan trong thực hiện công tác tuyên truyền, phổ biến giáo dục pháp luật về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu, giáo dục kỹ năng bảo vệ dữ liệu cá nhân, phòng, chống tội phạm lừa đảo chiếm đoạt tài sản và các hành vi vi phạm pháp luật khác trên không gian mạng (*nhiệm vụ thực hiện thường xuyên*).

7. Các cơ quan, đơn vị, địa phương

- Tập trung rà soát, đánh giá an ninh mạng, an toàn thông tin, an ninh dữ liệu đối với các hệ thống thông tin, cơ sở dữ liệu đang quản lý, vận hành, kịp thời phát hiện và khắc phục những điểm yếu, lỗ hổng bảo mật trên hệ thống thông tin (*hoàn thành trong tháng 4/2026*).

- Đánh giá thực trạng năng lực của đội ngũ cán bộ chuyên trách, hạ tầng công nghệ thông tin và chủ động bố trí nhân lực bảo đảm triển khai tổng thể các giải pháp giám sát, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các hệ thống thông tin trong phạm vi quản lý (*hoàn thành trong tháng 4/2026*).

- Phối hợp với Công an tỉnh và các đơn vị có liên quan để tổ chức thẩm định, phê duyệt cấp độ an toàn thông tin đối với toàn bộ các hệ thống thông tin trọng yếu do đơn vị trực tiếp quản lý, vận hành. Đối với hạ tầng và các hệ thống thông tin đang xây dựng hoặc sẽ triển khai trong thời gian tới, yêu cầu bắt buộc phải thực hiện phê duyệt cấp độ an toàn thông tin trước khi đưa vào vận hành chính thức. Đối với các hệ thống thông tin và hạ tầng hiện đang sử dụng, cần khẩn trương rà soát, đánh giá và thực hiện phê duyệt cấp độ an toàn thông tin theo đúng quy định (*hoàn thành trong tháng 4/2026*).

- Các đơn vị quản lý, vận hành các hệ thống thông tin quan trọng, hệ thống dùng chung của tỉnh phối hợp với Công an tỉnh rà soát, đánh giá an ninh mạng, an toàn thông tin, bảo mật dữ liệu trên các hệ thống thông tin, cơ sở dữ liệu và kịp thời bổ sung, khắc phục những tồn tại, hạn chế, nhất là khắc phục tình trạng "*nợ tuân thủ*" thiết bị, giải pháp bảo đảm an ninh mạng (*hoàn thành trong tháng 4/2026*).

- Phối hợp chặt chẽ với Công an tỉnh trong giám sát, điều phối ứng cứu, khắc phục sự cố về an toàn thông tin, an ninh mạng. Trong vòng 24 giờ kể từ khi xảy ra sự cố về an ninh mạng phải kịp thời báo cáo và tuân thủ điều phối ứng phó sự cố của Công an tỉnh - đơn vị chuyên trách về an toàn thông tin mạng tỉnh (*nhiệm vụ thực hiện thường xuyên*).

- Triển khai mô hình bảo đảm an toàn thông tin "04 lớp" gồm: (1) lực lượng tại chỗ chịu trách nhiệm vận hành, giám sát và ứng cứu ban đầu khi sự cố xảy ra; (2) hệ thống hoặc dịch vụ giám sát 24/7 giúp phát hiện sớm các nguy cơ; (3) đơn vị độc lập thực hiện kiểm tra, đánh giá định kỳ để bảo đảm khách quan và minh bạch; (4) kết nối, chia sẻ thông tin với hệ thống giám sát an ninh mạng tỉnh và hệ thống giám sát an ninh mạng quốc gia, bảo đảm sự phối hợp liên thông trên phạm vi toàn quốc (*hoàn thành trong tháng 4/2026*).

- Người đứng đầu các cơ quan, đơn vị có trách nhiệm lãnh đạo, chỉ đạo, kiểm tra và đôn đốc thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu. Chịu trách nhiệm trực tiếp và toàn diện nếu để xảy ra sự cố an ninh mạng nghiêm trọng, đặc biệt là lộ, lọt bí mật nhà nước do yếu tố chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định. Đưa kết quả đánh giá chỉ số bảo đảm an ninh mạng của các cơ quan, tổ chức vào tiêu chí đánh giá tín nhiệm, năng lực của cán bộ, nhất là đối với người đứng đầu, để phục vụ công tác xếp loại hằng năm. Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng nhằm củng cố lòng tin số của người dân trong quá trình hoạt động, tương tác và làm việc trên không gian mạng (*nhiệm vụ thực hiện thường xuyên*).

- Chủ động bố trí kinh phí trong dự toán chi ngân sách hàng năm và huy động các nguồn kinh phí hợp pháp khác để thực hiện công tác bảo đảm an toàn,

an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại cơ quan, đơn vị, địa phương (*nhiệm vụ thực hiện thường xuyên*).

Yêu cầu các đơn vị, địa phương liên quan tổ chức triển khai thực hiện nghiêm túc, hiệu quả Kế hoạch này. Quá trình thực hiện có khó khăn, vướng mắc, kịp thời phản ánh về Công an tỉnh để được hướng dẫn giải quyết. Định kỳ trước ngày 10/10 hằng năm, tổng hợp tình hình, kết quả thực hiện và những khó khăn, vướng mắc, báo cáo Ủy ban nhân dân tỉnh (*qua Công an tỉnh*) để tổng hợp.

Giao Công an tỉnh chủ trì theo dõi, đánh giá, hướng dẫn, đôn đốc các đơn vị, địa phương triển khai thực hiện Kế hoạch này. Hằng năm tổng hợp tình hình, kết quả thực hiện, đồng thời đề xuất khen thưởng, biểu dương, phê bình đối với các tập thể, cá nhân trong triển khai thực hiện Kế hoạch, báo cáo Bộ Công an, Ủy ban nhân dân tỉnh và cơ quan có thẩm quyền theo quy định. Chủ động báo cáo, tham mưu, đề xuất Ủy ban nhân dân tỉnh những nội dung đột xuất, phát sinh thuộc thẩm quyền./.

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Công an;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- Các đơn vị sự nghiệp,doanh nghiệp nhà nước thuộc UBND tỉnh;
- Đảng ủy, UBND các xã, phường;
- Chánh VP, các PCVP UBND tỉnh;
- Trung tâm CB - TH tỉnh;
- Lưu: VT, TH, VX, NC.

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

ỦY BAN NHÂN DÂN TỈNH HÀ TĨNH

Trần Báu Hà