

TỈNH ỦY NGHỆ AN
BAN CHỈ ĐẠO PHÁT TRIỂN
KHOA HỌC, CÔNG NGHỆ, ĐỔI MỚI
SÁNG TẠO, CHUYỂN ĐỔI SỐ,
CẢI CÁCH HÀNH CHÍNH
VÀ ĐỀ ÁN 06

ĐẢNG CỘNG SẢN VIỆT NAM

Nghệ An, ngày tháng 6 năm 2026

*
Số -KH/BCĐ

KẾ HOẠCH
bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu
trong hệ thống chính trị trên địa bàn tỉnh Nghệ An

Thực hiện 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 việc bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị (viết tắt là Kế hoạch số 04-KH/BCĐTW); Chương trình hành động số 24-CTr/TU, ngày 22/4/2026 của Tỉnh ủy về 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 Chỉ đạo về phát triển khoa học công nghệ, đổi mới sáng tạo, chuyển đổi số, cải cách hành chính và Đề án 06 tỉnh Nghệ An (sau đây gọi tắt là Ban Chỉ đạo tỉnh) ban hành Kế hoạch triển khai thực hiện như sau:

I- MỤC ĐÍCH, YÊU CẦU

1. Quán triệt, triển khai thực hiện nghiêm túc, kịp thời, thống nhất, hiệu quả các mục tiêu, yêu cầu, nhiệm vụ được giao tại Kế hoạch số 04-KH/BCĐTW, tạo chuyển biến mạnh mẽ trong nhận thức và hành động của các cấp ủy đảng, chính quyền và toàn hệ thống chính trị.

2. Đưa công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trở thành nhiệm vụ trọng yếu, thường xuyên của cả hệ thống chính trị nhằm bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh chính trị, trật tự an toàn xã hội, qua đó tạo môi trường số an toàn, tin cậy phục vụ chuyển đổi số, phát triển chính quyền số, kinh tế số, xã hội số; chủ động phòng ngừa, ngăn chặn nguy cơ tụt hậu, bị động trước các thách thức an ninh phi truyền thống, góp phần xây dựng tỉnh phát triển nhanh, bền vững trong kỷ nguyên số.

3. Xác định rõ các nhiệm vụ cụ thể của từng cơ quan, đơn vị trong việc triển khai thực hiện Kế hoạch; bảo đảm phân công rõ trách nhiệm, rõ tiến độ, rõ kết quả đầu ra.

II- MỤC TIÊU

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, bảo vệ vững chắc chủ quyền, an ninh và lợi ích của quốc gia trên không gian mạng, trong đó tập trung:

- Nâng cao hiệu quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong toàn bộ hệ thống chính trị của tỉnh; chủ động phòng ngừa, phát hiện, đấu tranh, ngăn chặn, xử lý kịp thời các nguy cơ, hành vi xâm phạm an ninh mạng; bảo vệ vững chắc hệ thống thông tin, cơ sở dữ liệu, bí mật nhà nước trên không gian mạng, phục vụ nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh trên địa bàn tỉnh.

- Nhận thức, kỹ năng cơ bản về an toàn thông tin, bảo vệ dữ liệu cá nhân được phổ biến rộng rãi trong xã hội; người dân, doanh nghiệp từng bước nâng cao khả năng phòng tránh các nguy cơ mất an toàn thông tin trên môi trường mạng.

- Tạo chuyển biến mạnh mẽ về nhận thức và trách nhiệm của các cấp ủy, chính quyền, cơ quan, đơn vị và đội ngũ cán bộ, đảng viên đối với công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

2. Mục tiêu cụ thể năm 2026

a) Về nhân lực an ninh mạng

Phấn đấu 50% lãnh đạo các cấp thuộc các cơ quan, đơn vị trong hệ thống chính trị, lực lượng vũ trang tỉnh Nghệ An và cán bộ chuyên trách công nghệ thông tin được tập huấn, bồi dưỡng nâng cao nhận thức về an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

b) Về an ninh mạng

- Hoàn thành rà soát, phân loại và phê duyệt cấp độ an toàn đối với 100% hệ thống thông tin các cơ quan, đơn vị, địa phương trong hệ thống chính trị và triển khai phương án bảo đảm an toàn theo cấp độ đã được phê duyệt.

- Nâng cao hiệu quả công tác giám sát và điều phối ứng cứu sự cố an ninh mạng.

- Hoàn thiện chủ trương thủ tục đầu tư xây dựng Trung tâm Giám sát An ninh mạng tỉnh.

c) Về bảo mật thông tin

- 100% cơ quan, đơn vị ban hành và tổ chức thực hiện quy chế bảo đảm

an ninh mạng, bảo mật thông tin và bảo vệ bí mật nhà nước trên môi trường mạng theo quy định.

- 100% hệ thống xử lý thông tin bí mật nhà nước được áp dụng giải pháp mật mã, ký số, mã hóa theo quy định; thực hiện kiểm soát truy cập, phân quyền và lưu vết truy cập.

d) Về an ninh dữ liệu

- Hoàn thành rà soát, phân loại dữ liệu dùng chung, dữ liệu chuyên ngành theo tính chất quan trọng của dữ liệu bảo đảm các yêu cầu về an ninh dữ liệu, các quy định về bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước.

- 100% dữ liệu quan trọng có biện pháp bảo vệ phù hợp được thực hiện sao lưu định kỳ và có phương án phục hồi khi xảy ra sự cố; bảo đảm nguyên tắc “an toàn ngay từ thiết kế” đối với các dự án công nghệ thông tin, chuyển đổi số mới.

3. Mục tiêu đến năm 2030

a) Về nhân lực an ninh mạng

- Phân đầu 100% lãnh đạo các cấp thuộc các cơ quan, đơn vị trong hệ thống chính trị, lực lượng vũ trang tỉnh Nghệ An được bồi dưỡng, cập nhật kiến thức về an ninh mạng và bảo vệ dữ liệu trong quá trình lãnh đạo, chỉ đạo chuyển đổi số.

- 100% cán bộ, công chức làm công tác chuyên trách, phụ trách về chuyển đổi số, an toàn thông tin, an ninh mạng tại các cơ quan Đảng, Nhà nước, MTTQ và các tổ chức chính trị - xã hội trên địa bàn tỉnh được đào tạo, bồi dưỡng chuyên sâu về an toàn thông tin, an ninh mạng, đủ năng lực quản trị, vận hành và bảo vệ hệ thống thông tin; 100% cán bộ, công chức làm việc với dữ liệu quan trọng, dữ liệu cá nhân được tập huấn kỹ năng nhận diện và phòng chống tấn công bằng công nghệ AI (*Deepfake, mã độc thế hệ mới...*).

- Xây dựng đội ngũ chuyên gia an ninh mạng trình độ cao của tỉnh có năng lực làm chủ công nghệ, đủ khả năng tham gia vận hành hiệu quả hệ thống giám sát an ninh mạng và xử lý các sự cố an ninh mạng phức tạp.

b) Về an ninh mạng

- Xây dựng và vận hành hiệu quả kiến trúc bảo vệ an ninh mạng tỉnh theo mô hình phòng thủ đa lớp, hiện đại, đồng bộ, phù hợp với kiến trúc bảo vệ an ninh mạng quốc gia; bảo đảm 100% hệ thống thông tin của các cơ quan Đảng, chính quyền, MTTQ và các tổ chức chính trị - xã hội trên địa bàn tỉnh được bảo vệ theo mô hình 4 lớp và được giám sát an toàn thông tin 24/7.

- Xây dựng Trung tâm Giám sát An ninh mạng tỉnh (*năm 2027: Triển khai xây dựng, lắp đặt hạ tầng, thiết bị vận hành*); duy trì Trung tâm Giám sát An ninh mạng tỉnh hoạt động ổn định, hiệu quả; thực hiện giám sát tập trung, kết nối, chia sẻ thông tin an ninh mạng đối với toàn bộ hệ thống thông tin quan trọng, cơ sở dữ liệu dùng chung và chuyên ngành.

- 100% các cơ quan trong hệ thống chính trị từ tỉnh đến xã, phường được triển khai đánh giá rủi ro an ninh mạng định kỳ hằng năm và áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia.

c) Về bảo mật thông tin

- 100% cơ quan, đơn vị thực hiện nghiêm quy chế bảo mật thông tin, bảo vệ bí mật nhà nước trên môi trường mạng; không để xảy ra lộ, mất bí mật nhà nước do nguyên nhân chủ quan.

- 100% hệ thống thông tin quan trọng áp dụng cơ chế xác thực đa yếu tố, phân quyền truy cập chặt chẽ, giám sát và kiểm soát truy cập bất thường.

d) Về an ninh dữ liệu

- Hoàn thành việc tập trung 100% dữ liệu dùng chung, dữ liệu chuyên ngành của tỉnh tại Trung tâm Dữ liệu tỉnh đạt chuẩn an ninh mạng.

- 100% dữ liệu quan trọng được mã hóa khi lưu trữ và truyền dẫn; được sao lưu, dự phòng và kiểm tra khả năng phục hồi định kỳ.

- Triển khai mô hình quản trị dữ liệu tập trung, bảo đảm dữ liệu được quản lý, khai thác, chia sẻ an toàn trong toàn bộ vòng đời, góp phần bảo đảm chủ quyền dữ liệu số của tỉnh.

e) Về phát triển sản phẩm, dịch vụ an ninh mạng nội địa

Phấn đấu đến năm 2030, trên 50% sản phẩm, dịch vụ an ninh mạng được đầu tư, mua sắm trong các dự án đầu tư công của tỉnh là sản phẩm “*Make in Vietnam*” đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng.

4. Tầm nhìn chiến lược đến năm 2045

Xây dựng môi trường không gian mạng an toàn, tin cậy; hình thành hệ sinh thái an ninh mạng của tỉnh với sự tham gia của doanh nghiệp công nghệ số trong nước; làm chủ công nghệ cốt lõi, giảm phụ thuộc nhập khẩu các sản phẩm, dịch vụ an ninh mạng; xây dựng đội ngũ chuyên gia, cán bộ kỹ thuật chất lượng cao; bảo đảm chủ động ứng phó với các thách thức về an ninh mạng trong bối cảnh chuyển đổi số toàn diện.

III- NHIỆM VỤ, GIẢI PHÁP

1. Tăng cường sự lãnh đạo, chỉ đạo; nâng cao nhận thức và trách nhiệm

- củng cố, kiện toàn Tiểu ban An ninh mạng tỉnh; phân công trách nhiệm

cụ thể cho từng thành viên; bảo đảm các nguồn lực, điều kiện để nâng cao hiệu quả hoạt động của Tiểu ban An ninh mạng tỉnh.

(Công an tỉnh chủ trì, phối hợp Văn phòng Tỉnh ủy và các cơ quan liên quan - thực hiện thường xuyên).

- Quán triệt, triển khai thực hiện nghiêm các chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; xác định đây là nhiệm vụ trọng yếu, cấp bách, thường xuyên của toàn hệ thống chính trị trên địa bàn tỉnh.

(Các cơ quan, đơn vị trong hệ thống chính trị - thực hiện thường xuyên).

- Ban hành các quy định, hướng dẫn về kiểm tra, đánh giá, bảo đảm an ninh mạng theo tiêu chuẩn TCVN 14423:2025 và các quy định của pháp luật hiện hành cho các cơ sở dữ liệu, hệ thống dùng chung trong hệ thống chính trị; định kỳ (6 tháng hoặc 01 năm) tổ chức kiểm tra, đánh giá việc thực hiện các quy định bảo đảm an ninh mạng, an toàn thông tin.

(Công an tỉnh chủ trì, phối hợp Văn phòng Tỉnh ủy và các cơ quan liên quan - thực hiện thường xuyên).

- Chủ trì, phối hợp các đơn vị có liên quan tham mưu UBND tỉnh rà soát, đánh giá toàn bộ các hệ thống hiện có để đề xuất nhu cầu sử dụng dịch vụ hạ tầng nhà trạm và nhu cầu sử dụng dịch vụ điện toán đám mây của Trung tâm Dữ liệu Quốc gia. Xây dựng lộ trình, kế hoạch chi tiết chuyển từng hệ thống thông tin lên Trung tâm Dữ liệu Quốc gia và Trung tâm Dữ liệu của tỉnh sau khi được xây dựng. Đầu tư, nâng cấp hạ tầng công nghệ thông tin đáp ứng yêu cầu và tuân thủ các quy định pháp lý hiện hành.

(Sở Khoa học và Công nghệ chủ trì, phối hợp với các cơ quan, đơn vị trong hệ thống chính trị thực hiện - hoàn thành trong Quý III/2026).

- Đưa tiêu chí đảm bảo an ninh mạng, bảo mật thông tin và an ninh dữ liệu vào đánh giá, xếp loại thi đua, khen thưởng của tổ chức, cơ quan, đơn vị, địa phương và người đứng đầu.

(Ban Tổ chức Tỉnh ủy, Sở Nội vụ chủ trì, phối hợp Công an tỉnh, Sở Khoa học và Công nghệ, các cơ quan, đơn vị trong hệ thống chính trị - thực hiện thường xuyên).

- Tổ chức tập huấn, bồi dưỡng nâng cao nhận thức về an ninh mạng, bảo mật thông tin, an ninh dữ liệu và trách nhiệm bảo đảm an toàn hệ thống thông tin theo cấp độ; phấn đấu trong năm 2026 đạt tối thiểu 50% lãnh đạo các cấp và cán bộ chuyên trách công nghệ thông tin được tập huấn; đến năm 2030 đạt 100% lãnh đạo các cấp và 100% cán bộ chuyên trách, phụ trách chuyển đổi số, an toàn thông tin, an ninh mạng được đào tạo, bồi dưỡng theo yêu cầu; 100%

cán bộ, công chức làm việc với dữ liệu quan trọng, dữ liệu cá nhân được tập huấn kỹ năng nhận diện và phòng, chống tấn công bằng công nghệ AI, Deepfake, mã độc thể hệ mới.

*(Công an tỉnh, Văn phòng Tỉnh ủy chủ trì, phối hợp Sở Khoa học và Công nghệ, Sở Nội vụ và các cơ quan liên quan - **thực hiện thường xuyên**).*

- Đẩy mạnh tuyên truyền, phổ biến, tập huấn kiến thức, kỹ năng an ninh mạng, bảo mật thông tin, bảo vệ dữ liệu cá nhân cho cán bộ, đảng viên, công chức, viên chức và Nhân dân; phát động phong trào toàn dân tham gia bảo vệ an ninh mạng.

*(Ban Tuyên giáo và Dân vận Tỉnh ủy; Báo và phát thanh, truyền hình Nghệ An chủ trì, phối hợp Công an tỉnh và các sở, ban, ngành, địa phương - **thực hiện thường xuyên**).*

- Triển khai các khóa đào tạo, phổ biến kỹ năng an ninh mạng cho cán bộ và người dân trên địa bàn tỉnh thông qua nền tảng “*Bình dân học vụ số*” và các nền tảng phù hợp khác.

*(Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ, Sở Giáo dục và Đào tạo và các cơ quan, đơn vị liên quan - **thực hiện thường xuyên**).*

- Nghiên cứu, triển khai các giải pháp định danh và đánh giá tín nhiệm mạng đối với tổ chức, cá nhân có ảnh hưởng trên không gian mạng, nhằm củng cố lòng tin số, nâng cao trách nhiệm của người dân khi hoạt động, tương tác và làm việc trên môi trường mạng.

*(Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ và các cơ quan, đơn vị liên quan - **thực hiện thường xuyên**).*

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

- Tham gia xây dựng, hoàn thiện, ban hành hoặc sửa đổi, bổ sung các quy chế, quy định về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; quy định về quản lý, vận hành, khai thác hệ thống thông tin, cơ sở dữ liệu; quy chế bảo vệ bí mật nhà nước trên không gian mạng.

*(Công an tỉnh, Văn phòng Tỉnh ủy chủ trì, phối hợp các cơ quan, đơn vị trong hệ thống chính trị thực hiện - **hoàn thành trong Quý III/2026**).*

- Các cơ quan, đơn vị trong hệ thống chính trị tỉnh rà soát, ban hành mới hoặc sửa đổi, bổ sung quy chế nội bộ về bảo đảm an ninh mạng, bảo mật thông tin, bảo vệ bí mật nhà nước trên môi trường mạng; hoàn thành trong năm 2026 và tổ chức thực hiện thường xuyên.

*(Các cơ quan, đơn vị trong hệ thống chính trị chủ trì, phối hợp Công an tỉnh, Văn phòng Tỉnh ủy, Sở Khoa học và Công nghệ thực hiện - **hoàn thành trong năm 2026 và tổ chức thực hiện thường xuyên**).*

- Thực hiện nghiêm quy định về xác định và phê duyệt cấp độ an toàn hệ thống thông tin và triển khai phương án bảo đảm an toàn thông tin theo cấp độ đã được phê duyệt; đồng thời đáp ứng yêu cầu bảo đảm an ninh mạng theo quy định; bảo đảm 100% hệ thống thông tin được triển khai phương án bảo đảm an toàn theo cấp độ đã được phê duyệt.

*(Các cấp ủy Đảng, chính quyền, MTTQ và các tổ chức chính trị - xã hội các cấp chủ trì, phối hợp Công an tỉnh thực hiện - **hoàn thành trong Quý II/2026**).*

- Yêu cầu các dự án ứng dụng công nghệ thông tin, chuyển đổi số phải có cấu phần an ninh mạng, bảo mật thông tin, an ninh dữ liệu được thẩm định trước khi triển khai; bảo đảm nguyên tắc “an toàn ngay từ thiết kế” đối với các hệ thống thông tin, cơ sở dữ liệu, nền tảng số mới.

*(Công an tỉnh, Sở Khoa học và Công nghệ chủ trì, Sở Tài chính phối hợp các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện thường xuyên**).*

- Áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia; thực hiện quản trị hệ thống dựa trên đánh giá rủi ro, tiêu chuẩn, quy chuẩn kỹ thuật; tổ chức đánh giá rủi ro an ninh mạng định kỳ hằng năm đối với hệ thống thông tin của các cơ quan trong hệ thống chính trị từ tỉnh đến xã, phường.

*(Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ và các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện thường xuyên**).*

- Thiết lập cơ chế phối hợp, chia sẻ thông tin, điều phối ứng cứu sự cố giữa các cơ quan, đơn vị và lực lượng chuyên trách an ninh mạng trên địa bàn tỉnh; xây dựng đầu mối tiếp nhận, cảnh báo, xử lý và báo cáo sự cố an ninh mạng, an toàn thông tin.

*(Công an tỉnh chủ trì, phối hợp các cơ quan, đơn vị trong hệ thống chính trị thực hiện - **hoàn thành trong Quý III/2026**).*

3. Bảo đảm an ninh mạng đối với hệ thống thông tin

- Triển khai đầy đủ mô hình bảo vệ 04 lớp; bảo đảm 100% hệ thống thông tin của các khối cơ quan Đảng, chính quyền, MTTQ và các tổ chức chính trị - xã hội trên địa bàn tỉnh được giám sát an toàn thông tin 24/7.

*(Công an tỉnh chủ trì, phối hợp Văn phòng Tỉnh ủy, các cơ quan, đơn vị trong hệ thống chính trị thực hiện - **hoàn thành trong Quý III/2026**).*

- Hoàn thiện hồ sơ, chủ trương, thủ tục đầu tư xây dựng Trung tâm Giám sát An ninh mạng tỉnh trong năm 2026; triển khai xây dựng, lắp đặt hạ tầng, thiết bị trong năm 2027; từng bước vận hành, mở rộng kết nối giám sát đến các hệ thống thông tin quan trọng, cơ sở dữ liệu dùng chung và chuyên ngành trong giai đoạn 2027 - 2030.

(Công an tỉnh chủ trì, phối hợp Văn phòng Tỉnh ủy, Sở Khoa học và Công nghệ, Sở Tài chính các cơ quan, đơn vị trong hệ thống chính trị thực hiện - hoàn thành trong Quý IV/2027).

- Rà soát, đánh giá, khắc phục lỗ hổng, điểm yếu an ninh mạng theo tiêu chuẩn TCVN 14423:2025; rà soát, kiểm tra an ninh đối với các thiết bị phần cứng, phần mềm và dịch vụ công nghệ thông tin do các đối tác bên thứ ba cung cấp, đặc biệt là các thiết bị có nguồn gốc từ nước ngoài hoặc sử dụng công nghệ mã nguồn đóng; định kỳ tổ chức kiểm tra, diễn tập, ứng cứu sự cố an ninh mạng.

(Công an tỉnh chủ trì, phối hợp các cơ quan, đơn vị trong hệ thống chính trị - thực hiện thường xuyên).

- Ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng “*Make in Viet Nam*”; ứng dụng trí tuệ nhân tạo, phân tích dữ liệu lớn và công nghệ tiên tiến trong giám sát, cảnh báo sớm và phòng thủ chủ động. Phát huy tối đa tiềm năng, trí tuệ Việt Nam gắn với tiếp thu, làm chủ và ứng dụng hiệu quả các thành tựu công nghệ, kỹ thuật tiên tiến của thế giới.

(Sở Khoa học và Công nghệ chủ trì, phối hợp Công an tỉnh, Sở Tài chính và các cơ quan, đơn vị trong hệ thống chính trị - thực hiện thường xuyên).

- Chủ động phối hợp với Bộ Công an để kết nối, tích hợp các hệ thống thông tin trọng yếu của tỉnh vào Hệ thống phòng vệ mạng quốc gia, nhằm tạo lá chắn bảo vệ từ xa, nâng cao năng lực phòng thủ vòng ngoài cho các hệ thống thông tin, tài nguyên trọng yếu trên Internet của tỉnh.

(Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ, các sở, ban, ngành liên quan - hoàn thành kết nối trong Quý III/2026, duy trì thường xuyên).

- Xây dựng và triển khai đồng bộ các giải pháp bảo vệ thiết bị đầu cuối trong các cơ quan, đơn vị, địa phương trong hệ thống chính trị trên địa bàn tỉnh; đồng thời tăng cường công tác tuyên truyền, trang bị kỹ năng bảo vệ người dùng trên không gian mạng, phòng, chống lừa đảo, xâm phạm dữ liệu cá nhân.

(Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ, Ban Tuyên giáo và Dân vận Tỉnh ủy, các cơ quan, đơn vị liên quan - thực hiện thường xuyên).

4. Tăng cường bảo mật thông tin và bảo vệ bí mật nhà nước trên không gian mạng

- Rà soát, phân loại thông tin theo các mức độ “*công khai, nội bộ, hạn chế, bí mật nhà nước*”; quản lý chặt chẽ việc soạn thảo, lưu trữ, truyền đưa, khai thác thông tin mật trên môi trường mạng.

(Công an tỉnh chủ trì, phối hợp Văn phòng Tỉnh ủy, Sở Khoa học và Công nghệ, các cơ quan, đơn vị trong hệ thống chính trị - thực hiện thường xuyên).

- Triển khai sử dụng đồng bộ giải pháp mật mã, chữ ký số, mã hóa dữ liệu trong trao đổi văn bản điện tử, xử lý công việc và lưu trữ thông tin bí mật nhà nước theo quy định.

*(Văn phòng Tỉnh ủy, Sở Khoa học và Công nghệ chủ trì, phối hợp Công an tỉnh, các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện thường xuyên**).*

- Quản lý chặt chẽ, bảo mật thiết bị, tài khoản, kiểm soát quyền truy cập hệ thống; thực hiện phân quyền, xác thực đa yếu tố, ghi nhật ký và giám sát truy cập đối với các hệ thống xử lý thông tin quan trọng, thông tin bí mật nhà nước.

*(Các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện thường xuyên**).*

- Tăng cường thanh tra, kiểm tra chuyên ngành; xử lý nghiêm các hành vi vi phạm quy định về bảo mật thông tin, để lộ, mất bí mật nhà nước trên môi trường mạng.

*(Công an tỉnh chủ trì, phối hợp Văn phòng Tỉnh ủy, Văn phòng Đoàn Đại biểu Quốc hội và HĐND tỉnh, Văn phòng UBND tỉnh, cơ quan Ủy ban MTTQ Việt Nam tỉnh, Sở Khoa học và Công nghệ - **thực hiện thường xuyên**).*

5. Bảo đảm an ninh dữ liệu và chủ quyền dữ liệu số của tỉnh

- Rà soát, phân loại dữ liệu dùng chung, dữ liệu chuyên ngành theo mức độ quan trọng, yêu cầu bảo vệ, phạm vi chia sẻ, khai thác; xác định danh mục dữ liệu quan trọng, dữ liệu cá nhân, dữ liệu thuộc phạm vi bí mật nhà nước để áp dụng biện pháp bảo vệ phù hợp.

*(Sở Khoa học và Công nghệ chủ trì, phối hợp Công an tỉnh, Văn phòng Tỉnh ủy và các cơ quan, đơn vị trong hệ thống chính trị thực hiện - **Hoàn thành trong năm 2026**).*

- Đẩy nhanh chuẩn hóa dữ liệu, phấn đấu đến Quý III/2026 hình thành Trung tâm Dữ liệu của tỉnh và đưa vào khai thác bước đầu; từng bước chuyển các hệ thống thông tin, dữ liệu dùng chung và chuyên ngành lên Trung tâm Dữ liệu Quốc gia và Trung tâm Dữ liệu của tỉnh. Giai đoạn 2028 - 2030, hoàn thiện tập trung 100% dữ liệu dùng chung và dữ liệu chuyên ngành, chấm dứt tình trạng lưu trữ phân tán, máy chủ không bảo đảm an toàn tại cấp cơ sở, phù hợp với lộ trình xây dựng Trung tâm Dữ liệu dùng chung của tỉnh.

*(Sở Khoa học và Công nghệ chủ trì, phối hợp các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện theo lộ trình 2026 - 2030**).*

- Ban hành và thực hiện quy chế quản lý, khai thác, chia sẻ và bảo vệ dữ liệu; xác định rõ trách nhiệm của cơ quan chủ quản dữ liệu và đơn vị vận hành hệ thống trong thu thập, cập nhật, khai thác, chia sẻ, lưu trữ, sao lưu, phục hồi và hủy bỏ dữ liệu.

*(Sở Khoa học và Công nghệ chủ trì, phối hợp các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện thường xuyên**).*

- Thực hiện sao lưu, dự phòng và phục hồi dữ liệu định kỳ; bảo đảm 100% dữ liệu quan trọng có phương án khôi phục khi xảy ra sự cố, tấn công mạng hoặc xảy ra thảm họa.

*(Các đơn vị chủ trì triển khai các hệ thống thông tin dùng chung của tỉnh, phối hợp Sở Khoa học và Công nghệ, Công an tỉnh và các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện thường xuyên**).*

- Bảo đảm nguyên tắc “*an toàn ngay từ thiết kế*” trong xây dựng cơ sở dữ liệu, nền tảng số; dữ liệu được bảo vệ trong toàn bộ vòng đời từ thu thập, xử lý, lưu trữ, chia sẻ đến hủy bỏ.

*(Các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện thường xuyên**).*

- Tăng cường kiểm soát, giám sát luồng dữ liệu kết nối liên thông; bảo đảm tính toàn vẹn, sẵn sàng và bí mật của dữ liệu trong mọi tình huống; kiểm tra định kỳ khả năng phục hồi dữ liệu đối với các hệ thống thông tin, cơ sở dữ liệu quan trọng.

*(Sở Khoa học và Công nghệ chủ trì, phối hợp Công an tỉnh và các cơ quan, đơn vị trong hệ thống chính trị - **thực hiện thường xuyên**).*

6. Phát triển nguồn nhân lực và tiềm lực an ninh mạng

- Kiện toàn nâng cao năng lực đội ngũ cán bộ chuyên trách an ninh mạng của Công an tỉnh, lực lượng thường trực bảo vệ an ninh mạng tại các cơ quan, đơn vị. Xây dựng đội ngũ chuyên gia an ninh mạng của tỉnh đủ năng lực làm chủ công nghệ, tham gia vận hành hiệu quả hệ thống giám sát an ninh mạng và xử lý các sự cố an ninh mạng phức tạp.

*(Công an tỉnh chủ trì, phối hợp Ban Tổ chức Tỉnh ủy, Văn phòng Tỉnh ủy, Sở Nội vụ thực hiện - **hoàn thành trong Quý IV/2026**).*

- Tăng cường liên kết giữa cơ quan nhà nước, cơ sở đào tạo và doanh nghiệp trong đào tạo, huấn luyện thực hành; xây dựng mạng lưới chuyên gia hỗ trợ ứng cứu sự cố an ninh mạng trên địa bàn tỉnh.

*(Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ, Sở Tài chính, Sở Giáo dục và Đào tạo - **thực hiện thường xuyên**).*

7. Bảo đảm nguồn lực tài chính, ngân sách

Bố trí kinh phí bảo đảm cho công tác an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo phân cấp ngân sách; ưu tiên đầu tư có trọng tâm, trọng điểm, tránh dàn trải. Bảo đảm tỷ lệ kinh phí bình quân chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu đạt tối thiểu 15% tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, chuyển đổi số. Hằng năm, hướng dẫn các cơ quan,

đơn vị, địa phương lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện nhiệm vụ bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo đúng quy định của pháp luật về ngân sách nhà nước.

(Sở Tài chính chủ trì, phối hợp các cơ quan, đơn vị trong hệ thống chính trị - thực hiện thường xuyên).

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

Tham gia góp ý xây dựng các khuôn khổ pháp lý, chuẩn mực chung của quốc tế khi có yêu cầu; chủ động triển khai thực hiện hiệu quả Công ước Hà Nội về chống tội phạm mạng năm 2025 và các điều ước, thỏa thuận quốc tế khác mà Việt Nam tham gia phù hợp với tình hình địa phương; tăng cường hợp tác chia sẻ thông tin, điều tra tội phạm mạng xuyên quốc gia.

(Công an tỉnh chủ trì, phối hợp Sở Ngoại vụ và các cơ quan, đơn vị liên quan - thực hiện thường xuyên).

9. Phát triển thị trường và hỗ trợ doanh nghiệp an ninh mạng trên địa bàn tỉnh

- Nghiên cứu, tham mưu ban hành các cơ chế, chính sách ưu đãi của tỉnh nhằm khuyến khích, hỗ trợ các doanh nghiệp công nghệ số, đặc biệt là doanh nghiệp khởi nghiệp sáng tạo trong lĩnh vực an ninh mạng, bảo mật thông tin; từng bước hình thành hệ sinh thái sản phẩm, dịch vụ an ninh mạng “*Make in Vietnam*” trên địa bàn.

(Sở Khoa học và Công nghệ chủ trì, phối hợp Sở Tài chính, Công an tỉnh và các sở, ngành liên quan - thực hiện thường xuyên).

- Hướng dẫn, theo dõi, tổng hợp tỷ lệ sử dụng sản phẩm, dịch vụ an ninh mạng “*Make in Vietnam*” trong các chương trình, đề án, dự án đầu tư công của tỉnh; định kỳ hằng năm báo cáo Ban Chỉ đạo tỉnh, phấn đấu đến năm 2030 đạt trên 50% sản phẩm, dịch vụ an ninh mạng được đầu tư, mua sắm trong các dự án đầu tư công của tỉnh là sản phẩm “*Make in Vietnam*”, đáp ứng các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng.

(Sở Khoa học và Công nghệ chủ trì, phối hợp Sở Tài chính, Công an tỉnh và các cơ quan, đơn vị liên quan - thực hiện thường xuyên).

IV- TỔ CHỨC THỰC HIỆN

1. Các cơ quan, đơn vị, địa phương các cấp trong hệ thống chính trị tỉnh căn cứ nội dung, nhiệm vụ được giao tại Kế hoạch này để xây dựng kế hoạch triển khai thực hiện nghiêm túc, hiệu quả, đúng thời gian, lộ trình quy định (có thể lồng ghép vào Kế hoạch thực hiện Chương trình hành động số 24-CTr/TU, ngày 22/4/2026 của Ban Thường vụ Tỉnh ủy Nghệ An về 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). Người đứng đầu 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.

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. Các cơ quan, đơn vị, địa phương trong hệ thống chính trị tỉnh căn cứ chức năng, nhiệm vụ được giao, tổ chức triển khai thực hiện Kế hoạch này và các văn bản, quy định của Tiểu ban An ninh mạng tỉnh đảm bảo tiến độ, chất lượng, yêu cầu; định kỳ 6 tháng (*trước ngày 05/6*) và hằng năm (*trước ngày 25/11*) báo cáo kết quả triển khai thực hiện Kế hoạch này về Ban Chỉ đạo tỉnh (qua Công an tỉnh) để tổng hợp, đánh giá.

3. Công an tỉnh chủ trì, theo dõi, đôn đốc việc triển khai thực hiện Kế hoạch này, kịp thời báo cáo Ban Chỉ đạo tỉnh, Tiểu ban An ninh mạng tỉnh các khó khăn, vướng mắc để chỉ đạo; đồng thời, định kỳ tổng hợp để tham mưu báo cáo cấp trên theo quy định. Chủ trì, phối hợp Văn phòng Tỉnh ủy, Sở Khoa học và Công nghệ và các cơ quan liên quan tham mưu triển khai các nhiệm vụ về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng, đánh giá rủi ro an ninh mạng, điều phối ứng cứu sự cố, kết nối Hệ thống phòng vệ mạng quốc gia, xây dựng và vận hành Trung tâm Giám sát An ninh mạng tỉnh. Thực hiện cập nhật, báo cáo định kỳ hằng tháng (trước ngày 25 hằng tháng) trên Hệ thống giám sát, đánh giá việc thực hiện Nghị quyết số 57-NQ/TW (<http://theodoinq.dcs.vn>) các nội dung về thực hiện công tác an ninh mạng, an ninh thông tin, an ninh dữ liệu theo phân công.

4. Sở Khoa học và Công nghệ chủ trì, phối hợp Công an tỉnh, Văn phòng Tỉnh ủy, Sở Tài chính và các cơ quan, đơn vị liên quan tham mưu triển khai các nhiệm vụ về hạ tầng công nghệ thông tin, Trung tâm Dữ liệu của tỉnh, chuyển đổi hệ thống thông tin lên Trung tâm Dữ liệu Quốc gia và Trung tâm Dữ liệu của tỉnh; hướng dẫn thực hiện nguyên tắc “an toàn ngay từ thiết kế” trong các dự án công nghệ thông tin, chuyển đổi số. Chủ trì, phối hợp các cơ quan liên quan rà soát, phân loại dữ liệu dùng chung, dữ liệu chuyên ngành; tham mưu ban hành quy chế quản lý, khai thác, chia sẻ và bảo vệ dữ liệu; hướng dẫn việc sao lưu, dự phòng, phục hồi dữ liệu, bảo đảm an ninh dữ liệu và chủ quyền dữ liệu số của tỉnh. Theo dõi, tổng hợp việc sử dụng sản phẩm, dịch vụ an ninh mạng “Make in Vietnam” trong các chương trình, đề án, dự án đầu tư công của tỉnh; phối hợp Sở Tài chính, Công an tỉnh tham mưu chính sách hỗ trợ, phát triển thị trường, doanh nghiệp công nghệ số, doanh nghiệp an ninh mạng trên địa bàn tỉnh.

5. Sở Tài chính, Văn phòng Tỉnh ủy chủ trì, phối hợp với các cơ quan, đơn vị liên quan tham mưu bố trí kinh phí từ ngân sách địa phương để triển khai các nhiệm vụ, giải pháp về bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu theo quy định; hằng năm hướng dẫn các cơ quan, đơn vị, địa phương lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện các nhiệm vụ bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo đúng quy định của pháp luật về ngân sách nhà nước. Phối hợp với các cơ quan liên quan tham mưu huy động, lồng ghép các nguồn lực hợp pháp khác để phục vụ triển khai các nhiệm vụ bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trên địa bàn tỉnh.

6. Ban Tổ chức Tỉnh ủy, Sở Nội vụ chủ trì, phối hợp Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan liên quan tham mưu đưa kết quả thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu vào tiêu chí đánh giá, xếp loại tổ chức, cơ quan, đơn vị, địa phương và người đứng đầu hằng năm. Phối hợp tham mưu kiện toàn tổ chức, bố trí, đào tạo, bồi dưỡng, nâng cao chất lượng đội ngũ cán bộ chuyên trách, phụ trách chuyên đổi số, an toàn thông tin, an ninh mạng tại các cơ quan, đơn vị trong hệ thống chính trị của tỉnh.

7. Ban Tuyên giáo và Dân vận Tỉnh ủy; Báo và phát thanh, truyền hình Nghệ An chủ trì, phối hợp Công an tỉnh, Sở Khoa học và Công nghệ, các cơ quan, đơn vị liên quan tổ chức tuyên truyền, phổ biến kiến thức, kỹ năng an ninh mạng, bảo mật thông tin, bảo vệ dữ liệu cá nhân cho cán bộ, đảng viên, công chức, viên chức, người dân và doanh nghiệp trên địa bàn tỉnh. Chủ động xây dựng chuyên trang, chuyên mục, tin, bài, phóng sự, tài liệu truyền thông về phòng, chống lừa đảo trên không gian mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, sử dụng dịch vụ số an toàn; phát động phong trào toàn dân tham gia bảo vệ an ninh mạng.

8. Sở Giáo dục và Đào tạo phối hợp Công an tỉnh, Sở Khoa học và Công nghệ, các cơ sở đào tạo và doanh nghiệp công nghệ số triển khai các chương trình đào tạo, tập huấn, phổ biến kỹ năng an ninh mạng cho cán bộ, giáo viên, học sinh, sinh viên và người dân thông qua nền tảng “Bình dân học vụ số” và các hình thức phù hợp khác. Phối hợp xây dựng, phổ biến tài liệu hướng dẫn kỹ năng nhận diện, phòng tránh lừa đảo trực tuyến, bảo vệ dữ liệu cá nhân, sử dụng Internet an toàn, văn minh.

9. Sở Ngoại vụ phối hợp Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan liên quan tham mưu, triển khai các nội dung hợp tác quốc tế trong lĩnh vực an ninh mạng, bảo mật thông tin, an ninh dữ liệu; chia sẻ thông tin, đào tạo, diễn tập và thực hiện các điều ước, thỏa thuận quốc tế mà Việt Nam tham gia, phù hợp với điều kiện thực tiễn của tỉnh.

10. Bộ Chỉ huy Quân sự tỉnh đảm bảo an ninh mạng, mật mã, bảo mật thông tin, an ninh dữ liệu trong lĩnh vực quân sự, quốc phòng, cơ yếu thuộc phạm vi quản lý của Bộ Quốc phòng; thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo phạm vi quản lý, chức năng, nhiệm vụ được giao.

11. Các doanh nghiệp viễn thông, công nghệ thông tin tham gia hoạt động chuyển đổi số tại các cơ quan, đơn vị, địa phương có trách nhiệm phối hợp chặt chẽ với Công an tỉnh và các cơ quan quản lý nhà nước thực hiện đầy đủ quy định pháp luật về đảm bảo an ninh mạng, an toàn thông tin, bảo vệ dữ liệu trong quá trình thiết kế, triển khai, vận hành hệ thống thông tin, nền tảng số, dịch vụ số.

Quá trình thực hiện nếu có khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương kịp thời báo cáo, đề xuất về Ban Chỉ đạo tỉnh (*qua Công an tỉnh*), để tổng hợp báo cáo Ban Chỉ đạo tỉnh xem xét, quyết định. Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ, Văn phòng Tỉnh ủy và các cơ quan liên quan định kỳ rà soát, đánh giá kết quả thực hiện Kế hoạch; trường hợp cần thiết tham mưu Ban Chỉ đạo tỉnh điều chỉnh, bổ sung nhiệm vụ, giải pháp cho phù hợp với tình hình thực tiễn và yêu cầu bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong từng giai đoạn.

Nơi nhận:

- BCD Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số (để báo cáo);
- Các đồng chí thành viên Ban Chỉ đạo tỉnh;
- Các đồng chí thành viên Tiểu ban An ninh mạng tỉnh;
- Các cơ quan chuyên trách, tham mưu giúp việc Tỉnh ủy;
- Thường trực HĐND tỉnh, UBND tỉnh, Ban Thường trực Ủy ban MTTQ Việt Nam tỉnh;
- Các ban, sở, ngành, đoàn thể cấp tỉnh; các đơn vị sự nghiệp công lập trực thuộc Tỉnh ủy;
- Các đảng ủy trực thuộc Tỉnh ủy; Đảng ủy, HĐND, UBND, UB MTTQ các xã, phường;
- Các doanh nghiệp viễn thông, CNTT (Viettel, VNPT, MobiFone Nghệ An);
- Công an tỉnh, Sở Nội vụ, Sở Khoa học và Công nghệ (các cơ quan thường trực Ban Chỉ đạo);
- Chánh, Phó Chánh Văn phòng Tỉnh ủy;
- Phòng Chuyển đổi số-Cơ yếu, VPTU;
- Lưu Văn phòng Tỉnh ủy.

PHÓ BÍ THƯ TỈNH ỦY
 kiêm
PHÓ TRƯỞNG BAN CHỈ ĐẠO

Võ Thị Minh Sinh