ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 107 /KH-UBND	*Hưng Yên, ngày 31 tháng 3 năm 2026*

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

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 *(gọi tắt là Ban Chỉ đạo Trung ương)*; Chương trình hành động số 09-CTr/TU ngày 13/02/2026 của 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; Ủy ban nhân dân tỉnh ban hành kế hoạch thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Quán triệt, triển khai thực hiện nghiêm túc, kịp thời, hiệu quả các quan điểm chỉ đạo, mục tiêu, yêu cầu, nhiệm vụ trong Kế hoạch số 04-KH/BCĐTW và các mục tiêu, nhiệm vụ, giải pháp, chỉ tiêu đã được giao trong Chương trình hành động số 09-CTr/TU.

- 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; là nền tảng quan trọng bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh chính trị, trật tự an toàn xã hội; 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.

2. Yêu cầu

- Xác định rõ các nhiệm vụ cụ thể của từng sở, ban, ngành; Đảng ủy, UBND các xã, phường trong việc triển khai thực hiện Kế hoạch; bảo đảm phân công rõ trách nhiệm, rõ tiến độ, rõ kết quả đầu ra; thực hiện đồng bộ, thống nhất, hiệu quả các nhiệm vụ về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh.

- Gắn bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu với quá trình chuyển đổi số của tỉnh; bảo đảm an toàn thông tin là điều kiện tiên quyết, xuyên suốt trong xây dựng chính quyền số, phát triển kinh tế số, xã hội số; không đánh đổi an toàn, an ninh mạng lấy tiến độ triển khai các ứng dụng, nền tảng số.

- Phát huy tối đa các nguồn lực, triển khai đồng bộ các nhiệm vụ, giải pháp đã đề ra; thực hiện rà soát hằng năm và tổ chức sơ kết, tổng kết theo định

kỳ 01 năm, 05 năm để đánh giá toàn diện kết quả thực hiện Kế hoạch; kịp thời điều chỉnh, bổ sung các nhiệm vụ, giải pháp phù hợp với tình hình thực tiễn, bảo đảm hoàn thành các mục tiêu đề ra.

- Việc triển khai thực hiện Kế hoạch phải gắn với các chương trình, kế hoạch của UBND tỉnh đã ban hành liên quan đến hoạt động khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trong tất cả các lĩnh vực.

II. MỤC TIÊU

1. Mục tiêu chung

Xây dựng không gian mạng quốc gia của tỉnh bảo đảm 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.

2. Mục tiêu cụ thể năm 2026

2.1. Về tổ chức, nhận thức

- 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; xác định đây là nhiệm vụ trọng yếu, thường xuyên của toàn hệ thống chính trị.

- 100% lãnh đạo sở, ban, ngành, cấp xã, phường 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.

2.2. Về an ninh mạng

- Hoàn thành rà soát, phân loại và phê duyệt cấp độ an toàn đối với 100% hệ thống thông tin của tỉnh và được 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; đề ra lộ trình xây dựng Trung tâm an ninh mạng tỉnh; 100% hệ thống thông tin quan trọng của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh được triển khai mô hình bảo vệ 4 lớp và được giám sát an toàn thông tin 24/7.

2.3. Về bảo mật thông tin

- 100% cơ quan, đơn vị ban hành và tổ chức thực hiện quy chế bảo đảm an toàn thông tin, bảo mật thông tin và bảo vệ bí mật nhà nước trên môi trường mạng.

- 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.

2.4. 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 và các quy định về bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước.

- 100% dữ liệu quan trọng 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

3.1. 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, Nhà nước trên địa bàn tỉnh được bảo vệ theo mô hình 4 lớp và được giám sát an toàn thông tin 24/7.

- Duy trì Trung tâm giám sát và điều hành 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 trên địa bàn tỉnh.

- 100% sở, ban, ngành, địa phương 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.

3.2. Về bảo mật thông tin

Duy trì 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, lọt 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.

3.3. 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; chấm dứt hoàn toàn tình trạng máy chủ phân tán, không bảo đảm an toàn tại cấp cơ sở.

- 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.

3.4. Về nhận thức, nhân lực an ninh mạng

- 100% lãnh đạo các sở, ban, ngành, UBND cấp xã, phường 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 chuyên trách, phụ trách công nghệ thông tin tại các cơ quan nhà nước 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...).

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

- Nhận thức và 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 và doanh nghiệp từng bước nâng cao khả năng phòng tránh các nguy cơ mất an toàn thông tin trên môi trường mạng.

4. Tầm nhìn chiến lược đến năm 2045

Góp phần 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; xây dựng đội ngũ chuyên gia, cán bộ kỹ thuật chất lượng cao; bảo đảm chủ động ứng phó với các thách thức 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

- Quán triệt, triển khai thực hiện nghiêm các chủ trương của Đảng, 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, thường xuyên của toàn hệ thống chính trị trên địa bàn tỉnh.

- Gắn trách nhiệm người đứng đầu cơ quan, đơn vị với kết quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; coi đây là tiêu chí đánh giá, xếp loại hằng năm.

- Tổ chức tập huấn, bồi dưỡng nâng cao nhận thức cho 100% lãnh đạo sở, ban, ngành, UBND cấp xã, phường và cán bộ chuyên trách công nghệ thông tin về an ninh mạng, bảo mật thông tin, an ninh dữ liệu và trách nhiệm bảo đảm an toàn hệ thống theo cấp độ.

- Đẩy mạnh tuyên truyền, phổ biến kiến thức, kỹ năng an toàn thông tin 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.

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

- Rà soát, tham mưu ban hành hoặc sửa đổi, bổ sung các quy chế, quy định về quy chế bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; 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.

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

- 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.

- 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.

- 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 trên địa bàn tỉnh.

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

- Triển khai đầy đủ mô hình bảo vệ 4 lớp; bảo đảm 100% hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh được giám sát an toàn thông tin 24/7.

- Xây dựng, nâng cấp và vận hành hiệu quả Hệ thống Trung tâm giám sát và điều hành an ninh mạng tỉnh; mở rộng kết nối giám sát đến các hệ thống thông tin quan trọng, cơ sở dữ liệu dùng chung và chuyên ngành.

- Rà soát, đánh giá, khắc phục lỗ hổng, điểm yếu an ninh mạng; rà soát, kiểm tra an ninh đối với các thiết bị phần cứng, phần mềm và dịch vụ CNTT 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.

- 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.

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 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.

- 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.

- Kiểm soát chặt chẽ 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.

- 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, lọt bí mật nhà nước.

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

- Hoàn thành tập trung 100% dữ liệu dùng chung và dữ liệu chuyên ngành của tỉnh tại Trung tâm dữ liệu tỉnh đạt chuẩn an ninh mạng; chấm dứt tình trạng lưu trữ phân tán, máy chủ không bảo đảm an toàn tại cấp cơ sở.

- 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.

- 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 thảm họa.

- 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.

- 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.

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

- Hình thành và kiện toàn đội ngũ chuyên trách an ninh mạng tại 100% sở, ban, ngành, UBND xã, phường. Xây dựng đội ngũ chuyên gia an ninh mạng của tỉnh đủ năng lực làm chủ công nghệ; 100% cán bộ chuyên trách công nghệ thông tin được đào tạo, bồi dưỡng chuyên sâu về an ninh mạng.

- 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.

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 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 và chuyển đổi số; đầu tư có trọng tâm, trọng điểm, tránh dàn trải, lãng phí.

- Thực hiện quy định ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng, an toàn thông tin "Make in Vietnam" đáp ứng yêu cầu bảo đảm an ninh mạng, bảo mật dữ liệu và an toàn thông tin bảo vệ an ninh mạng cho các cơ quan nhà nước trên địa bàn tỉnh.

8. Danh mục các nhiệm vụ giao các sở, ban, ngành địa phương *(chi tiết tại Phụ lục kèm theo)*.

IV. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành, đơn vị liên quan; UBND các xã, phường xây dựng kế hoạch triển khai thực hiện trước ngày 30/4/2026; 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 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 tỉnh; 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 10/11)*** báo cáo UBND tỉnh *(qua Công an tỉnh)* kết quả thực hiện, để tổng hợp, báo cáo theo quy định.

3. Sở Tài chính chủ trì, phối hợp với các sở, ngành, đơn vị liên quan tham mưu UBND tỉnh 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; hàng 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, an toàn thông tin và an ninh dữ liệu trên địa bàn tỉnh.

4. Giao Công an tỉnh chủ trì, phối hợp Sở Khoa học và Công nghệ và các sở, ngành, địa phương theo dõi, đôn đốc việc triển khai thực hiện Kế hoạch, kịp thời báo cáo và kiến nghị UBND tỉnh các biện pháp cần thiết để bảo đảm thực hiện đồng bộ và có hiệu quả Kế hoạch đồng thời tập hợp báo cáo theo quy định.

5. Quá trình triển khai, thực hiện, nếu có khó khăn, vướng mắc, các sở, ban, ngành, địa phương có văn bản gửi Công an tỉnh để tổng hợp và hướng dẫn giải quyết theo thẩm quyền hoặc trình cấp có thẩm quyền xem xét, quyết định./.

Nơi nhận:
- Thường trực: Tỉnh ủy, HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành, đoàn thể tỉnh;
- UBND các xã, phường;
- LĐVP UBND tỉnh;
- Lưu: VT, CVNC[Tường].

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

Nguyễn Lê Huy