UBND TỈNH NINH BÌNH
SỞ Y TẾ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 59 /KH-SYT

Ninh Bình, ngày 06 tháng 4 năm 2026

KẾ HOẠCH
Bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong Ngành Y tế tỉnh Ninh Bình

Thực hiện Kế hoạch số 100/KH-UBND ngày 01/4/2026 của UBND tỉnh về việc bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh Ninh Bình. Sở Y tế xây dựng kế hoạch triển khai thực hiện như sau:

I. MỤC TIÊU, YÊU CẦU

1. Mục tiêu chung

Tổ chức triển khai thực hiện hiệu quả, đạt mục tiêu các nội dung nhiệm vụ của địa phương tại Kế hoạch số 04-KH/BCĐTW của Ban Chỉ đạo Trung ương, nhằm xây dựng không gian mạng quốc gia 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 quốc gia trên không gian mạng.

2. Mục tiêu cụ thể

- Tạo chuyển biến mạnh mẽ, về nhận thức và hành động trong toàn bộ các đơn vị trực thuộc.

- Xây dựng và phát triển hạ tầng an ninh mạng hiện đại, đồng bộ, góp phần bảo vệ chủ quyền không gian mạng: (1) Các hệ thống thông tin của cơ quan, đơn vị, được rà soát, khắc phục các lỗ hổng, điểm yếu an ninh mạng; (2) Các hệ thống thông tin quan trọng thuộc danh mục được ưu tiên bảo vệ của đơn vị 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 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.

- Nâng cao nhận thức của cán bộ, đảng viên và người lao động về bảo mật thông tin, an ninh mạng và an ninh dữ liệu; đào tạo, bồi dưỡng đội ngũ chuyên gia an ninh mạng chất lượng cao.

- 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. Các hệ thống thông tin quan trọng được triển khai và áp dụng hiệu quả

Khung quản trị rủi ro an ninh mạng quốc gia. Ưu tiên, khuyến khích sử dụng dịch vụ an ninh mạng "Make in Vietnam" chiếm tỉ trọng trên 50%.

- 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 doạ mạng. Chuyển đổi sang mô hình phòng thủ chủ động, 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.

- Đến năm 2045, xây dựng nền an ninh mạng bền vững, tự chủ, có năng lực cạnh tranh.

3. Yêu cầu

- Bám sát các định hướng chỉ đạo đã nêu trong Kế hoạch số 04-KH/BCĐTW, bảo đảm tính đồng bộ, quyết liệt, có trọng tâm, trọng điểm.

- Phân công nhiệm vụ theo phương châm "6 rõ": Rõ người, rõ việc, rõ thời gian, rõ trách nhiệm, rõ sản phẩm, rõ thẩm quyền. 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. Gắn trách nhiệm người đứng đầu với kết quả bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

- Thường xuyên đôn đốc, kiểm tra, giám sát, kịp thời phát hiện, tháo gỡ các khó khăn, vướng mắc trong quá trình thực hiện.

II. CÁC NHIỆM VỤ, GIẢI PHÁP

1. Nhiệm vụ trọng tâm năm 2026

- Nêu cao vai trò, trách nhiệm của người đứng đầu, thủ trưởng cơ quan, đơn vị đối với công tác bảo đảm an toàn, an ninh mạng. Tổ chức 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.

- Tăng cường công tác giám sát an ninh mạng; phối hợp kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng với các hệ thống thông tin quan trọng của hệ thống chính trị từ cấp độ 3 trở lên (trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu).

- Triển khai thực hiện 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 trong hệ thống chính trị; định kỳ tổ chức kiểm tra, đánh giá việc thực hiện các quy định đảm bảo an ninh mạng, an toàn thông tin theo quy định.

2. Nhiệm vụ trọng tâm đến năm 2030

- Ban hành kế hoạch công tác, chương trình hoạt động hàng năm bám sát chỉ đạo của Trung ương, của tỉnh và định hướng phát triển của địa phương.

- Chú trọng nâng cao nhận thức cho toàn thể cán bộ, công chức, viên chức và người lao động đối với công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu. Tập trung thực hiện có hiệu quả phong trào "Bình dân học vụ số" và công tác đào tạo, bồi dưỡng, tuyên truyền phù hợp gắn với các hoạt động, tương tác trên không gian mạng.

- Xây dựng, 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. Quy hoạch và triển khai đồng bộ các nhóm giải pháp: Bảo vệ hạ tầng mạng, bảo vệ thiết bị đầu cuối, bảo vệ ứng dụng, dịch vụ, bảo vệ dữ liệu, bảo vệ người dùng. Bảo vệ tuyệt đối an toàn các hệ thống thông tin quan trọng, các cơ sở dữ liệu quốc gia. Kết nối, chia sẻ dữ liệu liên thông trên nguyên tắc bảo mật, an toàn, đúng pháp luật, khắc phục tình trạng cát cứ, phân mảnh dữ liệu.

- Bảo đảm về 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 tỉ 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% trong tổng kinh phí triển khai đềán, 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.

- Bảo đảm nguồn nhân lực an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại các cơ quan, đơn vị.

(Chi tiết các nhiệm vụ, giải pháp và phân công nhiệm vụ tại Phụ lục kèm theo Kế hoạch).

III. TỔ CHỨC THỰC HIỆN

1. Phòng Bảo hiểm Y tế

- Tiếp tục đẩy mạnh triển khai thực hiện hoàn thành các chỉ tiêu, yêu cầu, nhiệm vụ tại Đề án 06, đảm bảo gắn kết, đồng bộ với việc thực hiện các nội dung, nhiệm vụ của Kế hoạch này;

- Phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ theo dõi, đôn đốc việc thực hiện các nội dung của Kế hoạch; phối hợp với các cơ quan, đơn vị liên quan thực hiện tạo lập, triển khai ứng dụng hiệu quả các CSDL, hệ thống thông tin được giao chủ trì quản lý, vận hành.

2. Phòng Tài chính

Chủ trì, phối hợp với phòng Bảo hiểm y tế và các cơ quan, đơn vị có liên quan căn cứ vào tình hình thực tế trình nhu cầu kinh phí để triển khai thực hiện.

3. Văn phòng Sở

Chủ trì, phối hợp với các cơ quan, đơn vị liên quan triển khai đồng bộ các nhiệm vụ, giải pháp đảm bảo an toàn thông tin, an ninh mạng hệ thống mạng LAN tại Cơ quan Sở Y tế, Trang thông tin điện tử của Sở (*https://soyte.ninhbinh.gov.vn/)*.

4. Các đơn vị trực thuộc Sở Y tế

- Phối hợp chặt chẽ với đơn vị cung cấp dịch vụ CNTT và những cơ quan khác đảm bảo hiệu quả của việc trích chuyển dữ liệu sang cổng tiếp nhận dữ liệu của Bộ Y tế và cơ quan BHXH đảm bảo an toàn, bảo mật thông tin theo quy định;

- Nêu cao vai trò, trách nhiệm của người đứng đầu, thủ trưởng cơ quan, đơn vị đối với công tác bảo đảm an toàn, an ninh mạng. Tổ chức 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.

- Bảo đảm nguồn nhân lực an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại cơ quan, đơn vị và xây dựng, phát triển hạ tầng an ninh mạng hiện đại, đồng bộ, đáp ứng yêu cầu thực tế.

Đề nghị Thủ trưởng các đơn vị nghiêm túc triển khai các nội dung trong Kế hoạch, trong quá trình triển khai thực hiện có khó khăn, vướng mắc kịp thời báo cáo về Sở Y tế để phối hợp giải quyết./.

Nơi nhận:
- Lãnh đạo SYT;
- Công an tỉnh (để BC);
- Các đơn vị trực thuộc Sở Y tế;
- Các phòng chức năng Sở Y tế;
- Trang thông tin điện tử sở;
- Lưu VT, BHYT.

(MP/)

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ Y TẾ
TỈNH NINH BÌNH

Phan Anh Phong