UBND TỈNH ĐẮK LẮK **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 72 /KH-SYT	*Đắk Lắk, ngày 16 tháng 3 năm 2023*

KẾ HOẠCH
Triển khai thực hiện Quyết định số 964/QĐ-TTg của Thủ tướng Chính phủ về phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030

Thực hiện Kế hoạch số 37/KH-UBND ngày 07/03/2023 của UBND tỉnh về việc triển khai thực hiện Quyết định số 964/QĐ-TTg của Thủ tướng Chính phủ về phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030.

Sở Y tế xây dựng Kế hoạch triển khai thực hiện như sau:

I. MỤC TIÊU

1. Mục tiêu tổng quát

- Triển khai hiệu quả, đồng bộ các nội dung tại Quyết định số 964/QĐ-TTg nhằm có đủ điều kiện, tiềm lực tự chủ về an toàn, an ninh mạng, góp phần quan trọng trong bảo vệ sự thịnh vượng của Việt Nam trên không gian mạng.

- Xây dựng, phát triển văn minh, lành mạnh môi trường không gian mạng, tạo động lực tích cực để tham gia cuộc Cách mạng công nghiệp lần thứ tư, nâng cao năng lực về bảo đảm an toàn, an ninh mạng; chủ động, sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng nhằm bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng.

2. Mục tiêu cụ thể đến năm 2025

- Các cơ quan, đơn vị thực hiện tốt các quy định của pháp luật về bảo đảm thông tin và an ninh mạng.

- Bảo vệ cơ sở hạ tầng không gian mạng, trọng tâm là các hệ thống thông tin. Nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

- Tham mưu, đề xuất bổ sung nguồn kinh phí bảo đảm an toàn, an ninh mạng phục vụ cho việc nghiên cứu khoa học công nghệ, tin học, ứng dụng chuyển đổi số.

- Tham mưu, đề xuất xây dựng, hoàn thiện chính sách phù hợp, tạo điều kiện thuận lợi cho các doanh nghiệp trên địa bàn khởi nghiệp về lĩnh vực bảo đảm an toàn, an ninh mạng góp phần đặt nền móng hình thành nền công nghiệp an ninh mạng quốc gia.

3. Mục tiêu cụ thể đến năm 2030

- Duy trì, góp phần nâng cao năng lực thứ hạng về Chỉ số an toàn, an ninh

mạng. Xây dựng được thế trận an ninh nhân dân trên không gian mạng trên địa bàn với sự tham gia đông đảo, tích cực của quần chúng nhân dân.

- Từng bước hình thành các tổ, đội liên kết chặt chẽ trong công tác xử lý, ứng cứu sự cố thông tin về an ninh mạng; tăng cường lực lượng bảo đảm an toàn, an ninh mạng.

- Phấn đấu 90% cán bộ, công chức, viên chức và người lao động có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng xử lý các tình huống trên không gian mạng.

II. NHIỆM VỤ, GIẢI PHÁP

1. Tăng cường vai trò lãnh đạo của Đảng, quản lý của Nhà nước

- Thống nhất nhận thức từ cấp tỉnh tới cấp huyện/thị xã/thành phố về bảo đảm an toàn, an ninh mạng là trách nhiệm của cả hệ thống chính trị. Thường xuyên phổ biến, quán triệt chủ trương của Đảng, chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng, coi đây là nhiệm vụ quan trọng của hệ thống chính trị.

- Nâng cao nhận thức, trách nhiệm của các cấp ủy đảng, chính quyền, người dân, doanh nghiệp trong công tác bảo đảm an toàn, an ninh mạng. Người đứng đầu cấp ủy trực tiếp lãnh đạo, chỉ đạo và chịu trách nhiệm về công tác an toàn, an ninh mạng, chủ động rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo triển khai thực hiện các nhiệm vụ đạt hiệu quả.

- Phát huy sự tham gia của quần chúng nhân dân trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng.

2. Hoàn thiện hành lang pháp lý

- Tham gia xây dựng cơ chế, chính sách, pháp luật về an toàn, an ninh mạng và đội ngũ vận hành hệ thống thông tin quan trọng của Đảng, Nhà nước trên địa bàn.

3. Bảo vệ chủ quyền quốc gia trên không gian mạng

- Nghiên cứu, đề xuất ban hành các quy định về bảo vệ chủ quyền quốc gia trên không gian mạng phù hợp với tình hình thực tế trên địa bàn và chức năng, nhiệm vụ của cơ quan, đơn vị.

- Xây dựng năng lực tự chủ, phản ứng trước các hoạt động xâm phạm chủ quyền quốc gia trên không gian mạng.

4. Bảo vệ hạ tầng số, nền tảng số, dữ liệu số, cơ sở hạ tầng không gian mạng quốc gia

a) Bảo vệ cơ sở hạ tầng không gian mạng quốc gia trên địa bàn

- Bảo đảm an toàn, an ninh mạng trong quá trình lựa chọn, triển khai các dịch vụ, công nghệ cho cơ sở hạ tầng không gian mạng; ưu tiên sử dụng sản phẩm an toàn, an ninh mạng Việt Nam.

- Bảo đảm an toàn, an ninh mạng trong quá trình thiết kế, xây dựng, vận hành, khai thác cơ sở hạ tầng không gian mạng. Giám sát, cảnh báo sớm các hành vi vi phạm pháp luật trên không gian mạng.

- Bảo đảm an toàn, an ninh mạng cho quá trình triển khai Chính phủ điện tử, chuyển đổi số.

b) Bảo vệ hạ tầng số

- Lựa chọn sử dụng dịch vụ viễn thông, Internet và dịch vụ hạ tầng số được công khai mức độ an toàn, an ninh mạng. Ưu tiên sử dụng sản phẩm an toàn, an ninh mạng "Make in Viet Nam".

- Chủ động thông báo cho lực lượng chức năng khi phát hiện các hành vi vi phạm pháp luật trên không gian mạng; thực hiện hoặc thông báo, phối hợp với doanh nghiệp hạ tầng số khắc phục, xử lý hoặc từng bước thay thế thiết bị đầu cuối có dấu hiệu mất an toàn thông tin mạng.

c) Bảo vệ nền tảng số

- Chủ động giám sát, phát hiện và công bố hành vi vi phạm quy định pháp luật thuộc phạm vi quản lý trên các nền tảng số. Xử lý theo thẩm quyền hoặc phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông xử lý tổ chức, cá nhân vi phạm, gỡ bỏ thông tin vi phạm trên các nền tảng số.

5. Bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước

- Nâng cao trách nhiệm tự bảo vệ hệ thống thông tin thuộc phạm vi quản lý. Gắn trách nhiệm của người đứng đầu cơ quan chủ quản hệ thống thông tin với trách nhiệm bảo đảm an toàn, an ninh mạng.

- Xây dựng, cập nhật, vận hành hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng.

- Rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

- Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng.

- Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá trình thi công, lắp đặt thiết bị trong các hệ thống thông tin.

- Đầu tư nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức và người lao động. Phối hợp với cơ quan chuyên trách về an ninh mạng của Công an tỉnh để kết nối với Trung tâm An ninh mạng cấp tỉnh để giám sát an ninh mạng trên địa bàn.

6. Bảo vệ hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin

- Triển khai phương án bảo đảm an toàn thông tin theo cấp độ và mô hình bảo vệ 4 lớp đối với hệ thống thông tin của các lĩnh vực quan trọng.

- Ưu tiên sử dụng sản phẩm, giải pháp an toàn thông tin mạng "Make in Viet Nam" trong các hệ thống thông tin quan trọng quốc gia.

- Nâng cao nhận thức cho các tổ chức, cá nhân liên quan về bảo đảm an toàn thông tin mạng cho các hệ thống thông tin của các lĩnh vực quan trọng.

7. Tạo lập niềm tin số, xây dựng môi trường mạng trung thực, văn minh, lành mạnh và phòng, chống vi phạm pháp luật trên không gian mạng

- Giám sát, phát hiện và phối hợp với cơ quan chức năng và các doanh nghiệp nền tảng số xử lý tin giả, thông tin vi phạm pháp luật trong phạm vi quản lý.

- Phát triển các website, trang mạng xã hội, tài khoản trên môi trường mạng uy tín, nhiều tương tác để tuyên truyền, định hướng thông tin, dư luận và phản bác hiệu quả các thông tin tiêu cực về đất nước, con người Việt Nam.

8. Đào tạo và phát triển nguồn nhân lực

- Tích cực tham gia triển khai Đề án "Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025"; nghiên cứu, đề xuất phương án thúc đẩy hoạt động trong lĩnh vực này giai đoạn 2026 - 2030.

9. Tuyên truyền, phổ biến, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng

- Tăng cường các hoạt động tuyên truyền, nâng cao nhận thức và phổ biến kiến thức, trang bị kỹ năng bảo đảm an toàn thông tin tới toàn thể người sử dụng Internet; triển khai hoạt động trang bị kỹ năng cho các nhóm người yếu thế, dễ bị tổn thương trong xã hội.

- Cung cấp kịp thời các thông tin chính thống để người dân nắm bắt, cùng phản biện tin giả, thông tin vi phạm pháp luật trên môi trường mạng.

- Trong phạm vi quản lý, tổ chức triển khai các kế hoạch tuyên truyền, phổ biến về thói quen, trách nhiệm, kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức, người lao động khi tham gia hoạt động trên không gian mạng.

10. Đầu tư nguồn lực và bảo đảm kinh phí thực hiện

- Bố trí đủ nhân lực chuyên trách, chịu trách nhiệm về an toàn, an ninh mạng trong các cơ quan, đơn vị.

- Đầu tư nguồn lực để xây dựng hệ thống kỹ thuật, công cụ và triển khai các hoạt động bảo đảm an toàn, an ninh mạng và trong hoạt động của các cơ quan, đơn vị.

- Bố trí kinh phí chi cho an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho khoa học công nghệ, chuyển đổi số, ứng dụng công nghệ thông tin.

- Phân bổ ngân sách bảo đảm kinh phí thực hiện các nhiệm vụ theo nội dung Kế hoạch.

III. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở Y tế

- Chủ trì, phối hợp, hướng dẫn, đôn đốc, kiểm tra các cơ quan, đơn vị triển khai thực hiện các nội dung về an toàn thông tin mạng tại Kế hoạch này; đề xuất, kiến nghị nhiệm vụ mới cho phù hợp với tình hình thực tiễn đối với các nội dung về an toàn thông tin mạng thuộc Kế hoạch.

2. Các tổ chức TMTH-CMNV Sở Y tế

- Chủ động, tích cực phối hợp triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động và phạm vi quản lý.

3. Các cơ quan, đơn vị trực thuộc Sở Y tế

- Đẩy mạnh hoạt động bảo đảm an toàn, an ninh mạng trong phạm vi quản lý; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật theo quy định của pháp luật. Gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác triển khai chuyển đổi số, ứng dụng công nghệ thông tin, phát triển Chính phủ điện tử hướng tới Chính phủ số, phát triển đô thị thông minh, kinh tế số và xã hội số.

- Chủ động rà soát, phát hiện và xử lý, hoặc phối hợp với cơ quan chức năng có thẩm quyền xử lý thông tin vi phạm pháp luật trên môi trường mạng thuộc phạm vi quản lý.

- Rà soát, đánh giá, có biện pháp tăng cường bảo đảm an toàn, an ninh mạng đối với các hệ thống hạ tầng thông tin, hệ thống thông tin do cơ quan, đơn vị quản lý, vận hành, khai thác.

- Ưu tiên bố trí nguồn lực (nhân lực, kinh phí) và điều kiện để triển khai hoạt động bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, đơn vị và lĩnh vực quản lý.

- Thực hiện báo cáo hàng năm ***(trước ngày 05/10)*** hoặc đột xuất về tình hình, kết quả triển khai thực hiện Kế hoạch gửi về Sở Y tế để tổng hợp, báo cáo theo quy định.

Trên đây là Kế hoạch triển khai thực hiện Quyết định số 964/QĐ-TTg của Thủ tướng Chính phủ về phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030./.

Nơi nhận:
- Giám đốc, các PGĐ Sở Y tế;
- Các tổ chức TMTH-CMNV Sở Y tế;
- Các cơ quan, đơn vị trực thuộc Sở Y tế;
- Lưu: VT, VP (N, 01b).

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH ĐẮK LẮK

Nay Phi La