UBND TỈNH NINH THUẬN **SỞ Y TẾ** Số: 1733 /SYT-KHNVTC	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *Ninh Thuận, ngày 02 tháng 5 năm 2024*

V/v tăng cường bảo đảm an toàn hệ thống thông tin mạng.

Kính gửi: Các đơn vị trực thuộc.

Thực hiện Công văn số 2132/BYT-K2ĐT ngày 26/4/2024 của Bộ Y tế về tăng cường bảo đảm an toàn hệ thống thông tin mạng.

Trước tình hình hoạt động tấn công mạng ngày càng tăng và phức tạp, đặc biệt là hình thức tấn công mã độc (Ransomeware) và có thể tiếp tục diễn biến với quy mô đột biến và tính chất gia tăng trong thời gian tới. Sở Y tế đã có nhiều văn bản chỉ đạo về tăng cường bảo đảm an toàn thông tin, an ninh mạng. Tuy nhiên, một số đơn vị trong ngành chưa quán triệt, ưu tiên nguồn lực triển khai, vẫn để xảy ra sự cố gây mất an toàn thông tin, an ninh mạng như một số trang thông tin điện tử, hệ thống thông tin tồn tại nhiều điểm yếu, lỗ hổng bảo mật, lộ tài khoản trên không gian mạng, bị tin tặc tấn công, chèn thông tin xấu độc.

Sở Y tế yêu cầu các đơn vị khẩn trương tập trung thực hiện những nội dung trọng tâm sau:

1. Thủ trưởng Đơn vị trực tiếp chỉ đạo và phụ trách công tác đảm bảo an toàn thông tin, an ninh mạng, ưu tiên nguồn lực, khẩn trương, quyết liệt triển khai có hiệu quả công tác này, chịu trách nhiệm trước pháp luật và cơ quan có thẩm quyền nếu để hệ thống thông tin thuộc phạm vi quản lý không đảm bảo an toàn thông tin, an ninh mạng, để xảy ra sự cố nghiêm trọng.

2. Quán triệt, thực hiện nghiêm Luật An toàn thông tin mạng, Luật An ninh mạng, Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phu quy định chi tiết một số điều Luật An ninh mạng, Nghị định số 13/2023/NĐ-CP ngày 17/4/2024 của Chính phủ về bảo vệ dữ liệu cá nhân, Nghị định số 85/2016/NĐ-CP ngày 15/8/2022 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ (Nghị định số 85/2016/NĐ-CP), Chỉ thị số 09/CT- TTg, các quy định, chỉ đạo, hướng dẫn khác về an toàn thông tin, an ninh mạng; Cụ thể hóa trách nhiệm của đơn vị, tổ chức, cá nhân trong công tác bảo vệ an ninh mạng hệ thống thông tin trọng yếu, bảo vệ dữ liệu cá nhân.

3. Xây dựng, trình cơ quan có thẩm quyền để thẩm định, phê duyệt hồ sơ đề xuất cấp độ an toàn thông tin đối với 100% hệ thống thông tin thuộc phạm vi quản lý theo quy định tại Nghị định số 85/2016/NĐ-CP và các văn bản quy

phạm pháp luật có liên quan; thực hiện nghiêm thời hạn hoàn thành phê duyệt hồ sơ đề xuất cấp độ an toàn thông tin, triển khai đầy đủ phương án bảo đảm an toàn thông tin như hồ sơ đề xuất cấp độ đã được phê duyệt theo đúng chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 09/CT-TTg ngày 23/02/2024.

4. Các đơn vị có cung Cấp dịch vụ trực tuyến phục vụ người dân, doanh nghiệp phải tăng cường đảm bảo an toàn thông tin, an ninh mạng, tuân thủ đầy đủ quy định của pháp luật về an toàn thông tin, an ninh mạng, đặc biệt quy định về đảm bảo an toàn thông tin theo cấp độ.

5. Xây dựng kế hoạch ứng phó sự cố đối với hệ thống thông tin thuộc phạm vi quản lý theo quy định tại Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc. Triển khai phương án sao lưu định kỳ hệ thống và dữ liệu quan trọng để kịp thời khôi phục khi bị tấn công mã hóa dữ liệu và báo cáo sự cố về cơ quan quản lý an toàn thông tin, an ninh mạng trực tiếp theo quy định.

6. Sử dụng thường xuyên các nền tảng hỗ trợ đảm bảo an toàn thông tin do Bộ Thông tin và Truyền thông cung cấp để nâng cao hiệu quả hoạt động quản lý và thực thi pháp luật về an toàn thông tin mạng.

7. Bố trí hạng mục về an toàn thông tin mạng khi xây dựng, triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm, giai đoạn 5 năm và dự án công nghệ thông tin; bảo đảm tỷ lệ kinh phí chi cho các sản phẩm, dịch vụ an toàn thông tin mạng đạt tối thiểu 10% tổng kinh phí triển khai các kế hoạch, dự án này theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 14/CT-TTg ngày 07/6/2019.

8. Thường xuyên tập huấn, bồi dưỡng, nâng cao kiến thức, kỹ năng cho công chức, viên chức, người lao động, đội ngũ cán bộ chuyên trách công nghệ thông tin, an toàn thông tin, an ninh mạng đáp ứng năng lực, yêu cầu bảo đảm an toàn thông tin, an ninh mạng và bảo vệ bí mật nhà nước trên không gian mạng.

9. Trường hợp xảy ra sự cố bị tấn công mạng, cần tuân thủ nghiêm túc quy định và chỉ đạo tại Quyết định số 05/2017/QĐ-TTG ngày 16/03/2017, Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ, Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông, lưu ý một số nội dung trọng tâm sau:

a) Kịp thời báo cáo sự cố về cơ quan chủ quản, đơn vị chuyên trách ứng cứu sự cố cùng cấp và cấp trên, Bộ Y tế, Cơ quan điều phối quốc gia, các cơ quan, doanh nghiệp có chức năng quản lý an ninh mạng.

b) Tuân thủ sự điều phối ứng cứu sự cố của Cơ quan điều phối quốc gia và các cơ quan chức năng liên quan trong việc: thu thập, phân tích thông tin; xử lý, khắc phục sự cố; xác minh nguyên nhân và truy tìm nguồn gốc; phát ngôn và công bố thông tin,...

c) Báo cáo đầy đủ về thông tin sự cố, thiệt hại và các thông tin liên quan, đồng thời tổng kết, phân tích, đánh giá, rút ra bài học và báo cáo về Cơ quan điều phối quốc gia để tổng hợp, phổ biến và cơ quan quản lý có thẩm quyền.

Đầu mối liên hệ, hỗ trợ: ThS. Trần Văn Tuyên - Phòng Quản lý Công nghệ thông tin y tế - Cục Khoa học công nghệ và Đào tạo, Bộ Y tế; Điện thoại: 0934.575.477; Email: tuyentv.k2dt@moh.gov.

Sở Y tế yêu cầu Thủ trưởng các đơn vị khẩn trương triển khai thực hiện đúng quy định./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Website Sở Y tế;
- Lưu: VT, KHNVTC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH NINH THUẬN

Bùi Văn Kỳ