UBND TỈNH BÀ RỊA-VŨNG TÀU **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 3187 /SYT-KHTC V/v triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2024.	*Bà Rịa-Vũng Tàu, ngày 12 tháng 08 năm 2024*

Kính gửi:

- Các phòng chuyên môn, nghiệp vụ Sở Y tế;
- Các cơ quan, đơn vị trực thuộc Sở Y tế;

(dưới đây gọi tắt là đơn vị)

Thực hiện Công văn số 4963/UBND-VP ngày 17/4/2024 của Ủy ban nhân dân tỉnh, về việc triển khai một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2024, Sở Y tế đề nghị Thủ trưởng các đơn vị nghiêm túc triển khai thực hiện một số nhiệm vụ trọng tâm về an toàn thông tin mạng trong năm 2024 như sau:

1. Nghiêm túc tiếp tục triển khai thực hiện Kế hoạch số 13/KH-UBND ngày 10/02/2023 của Ủy ban nhân dân tỉnh về việc triển khai thực hiện Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ 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" (đính kèm);

2. Bảo đảm an toàn hệ thống thông tin theo cấp độ

- Người đứng đầu đơn vị trực tiếp chỉ đạo và ưu tiên nguồn lực để tổ chức thực thi, triển khai công tác bảo đảm an toàn hệ thống thông tin theo cấp độ theo chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 09/CT-TTg ngày 23/02/2024 và Công điện số 33/CĐ-TTg ngày 07/4/2024.

- Áp dụng hiệu quả Sổ tay Hướng dẫn bảo đảm an toàn hệ thống thông tin theo cấp độ được ban hành tại Công văn số 478/CATTT-ATHTTT ngày 30/3/2024 của Cục An toàn Thông tin - Bộ Thông tin và Truyền thông (đã được Sở Thông tin và Truyền thông triển khai tại Công văn số 708/STTTT-CĐSBCVT ngày 10/4/2024).

- Thường xuyên sử dụng hiệu quả Nền tảng Hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ đã được Bộ Thông tin và Truyền thông cung cấp cấp miễn phí (đã được Sở Thông tin và Truyền thông hướng dẫn sử dụng tại Công văn số 712/STTTT-CĐSBCVT ngày 11/4/2024).

- Tập trung rà soát, hoàn thành việc phân loại, xác định và phê duyệt Hồ sơ đề xuất cấp độ đối với 100% hệ thống thông tin đang vận hành **chậm nhất trong tháng 9 năm 2024.**

- Triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ được phê duyệt cho 100% hệ thống thông tin đang vận hành **chậm nhất trong tháng 12 năm 2024**. Căn cứ Hồ sơ đề xuất cấp độ và phương án bảo đảm an toàn hệ thống thông tin đã được phê duyệt, đề nghị tổ chức rà soát, đánh giá và triển khai phương án bảo đảm an toàn thông tin, bảo đảm các yêu cầu quản lý, yêu cầu kỹ thuật đều được đáp ứng, đặc biệt là các yêu cầu chưa đáp ứng tại thời điểm phê duyệt Hồ sơ đề xuất cấp độ.

- Đối với các hệ thống thông tin đầu tư mới hoặc mở rộng, nâng cấp, khuyến nghị xây dựng và phê duyệt Hồ sơ đề xuất cấp độ trước khi phê duyệt Báo cáo nghiên cứu khả thi (hoặc hồ sơ tương đương) và triển khai phương án bảo đảm an toàn thông tin đã được phê duyệt tại Hồ sơ đề xuất cấp độ trước khi đưa vào vận hành, khai thác theo quy định tại khoản 6 Điều 9 Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Duy trì và nâng cao hiệu quả công tác bảo đảm an toàn thông tin theo mô hình "4 lớp"

- 100% hệ thống thông tin của cơ quan, tổ chức được duy trì và nâng cao hiệu quả tổ chức bảo đảm an toàn thông tin theo mô hình "4 lớp" (Lực lượng tại chỗ; Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp; Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia), đặc biệt là nâng cao năng lực của lớp giám sát, bảo vệ chuyên nghiệp và kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

- Về lực lượng tại chỗ: tổ chức, kiện toàn lực lượng tại chỗ theo hướng chuyên nghiệp, cơ động thông qua hoạt động đào tạo, tuyển dụng hoặc thuê ngoài chuyên gia. Tích cực khai thác, sử dụng Nền tảng điều phối xử lý sự cố an toàn thông tin mạng quốc gia tại địa chỉ irlab.vn trong công tác báo cáo sự cố, ứng cứu sự cố, huấn luyện, diễn tập để nâng cao năng lực cán bộ và được hỗ trợ khi xảy ra sự cố an toàn thông tin mạng (đã được Sở Thông tin và Truyền thông triển khai tại Công văn số 842/STTTT-VTCNTT ngày 09/5/2023).

- Về giám sát, bảo vệ chuyên nghiệp: hoàn thành mở rộng phạm vi giám sát, bảo vệ cho 100% hệ thống thông tin thuộc phạm vi quản lý **chậm nhất**

trong tháng 11 năm 2024. Đối với các hệ thống thông tin cấp độ 3 trở lên phải tổ chức giám sát, bảo vệ đầy đủ các lớp: lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu, lớp thiết bị đầu cuối.

- Về kiểm tra, đánh giá định kỳ: kiểm tra, đánh giá an toàn thông tin định kỳ theo quy định tại Điều 20 Nghị định số 85/2016/NĐ-CP cho tối thiểu 80% hệ thống thông tin thuộc phạm vi quản lý; 100% hệ thống thông tin cấp độ 3 trở lên được kiểm tra, đánh giá an toàn thông tin định kỳ hàng năm. Rà soát danh sách các webiste *.baria-vungtau.gov.vn, bao gồm cả các sub domain để tiến hành đánh giá an toàn thông tin định kỳ và triển khai gán nhãn tín nhiệm mạng cho các webiste.

- Về kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia: duy trì kết nối ổn định, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực về Hệ thống giám sát quốc gia để được hỗ trợ giám sát, phân tích, cảnh báo sớm các nguy cơ về an toàn thông tin mạng và tấn công mạng.

3. Kiểm tra tuân thủ quy định của pháp luật về an toàn thông tin mạng

- Nhận thức đầy đủ theo đánh giá của Bộ Thông tin và Truyền thông: *"Bảo đảm an toàn thông tin mạng vừa là bảo vệ tổ chức, nhưng cũng là trách nhiệm của tổ chức. Nếu không tuân thủ, tổ chức sẽ phải đối mặt với rủi ro và chịu trách nhiệm trước pháp luật khi xảy ra sự cố. Theo Luật, an toàn thông tin mạng là yêu cầu "bắt buộc", không phải là yếu tố để "lựa chọn". Tuy nhiên, nhiều cơ quan chưa nhận thức hoặc nhận thức chưa đầy đủ vấn đề này. Vì vậy, nhận thức và mức độ tuân thủ các quy định về bảo đảm an toàn thông tin của các đơn vị trực thuộc các bộ, ngành, địa phương còn lỏng lẻo, hạn chế, chưa được quan tâm thực hiện đầy đủ. Đây là một trong những nguyên nhân cơ bản khiến cho nguy cơ mất an toàn thông tin trong hoạt động của cơ quan, tổ chức còn nhiều vấn đề đáng lo ngại".*

- Tự kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an toàn thông tin mạng đối với hệ thống thông tin trong phạm vi quản lý đã được phê duyệt cấp độ an toàn hệ thống thông tin.

4. Sử dụng hiệu quả các nền tảng số

- 100% các sở, ban, ngành, địa phương triển khai áp dụng hiệu quả các nền tảng được cung cấp để thực hiện quản lý nhà nước và thực thi pháp luật trong phạm vi quản lý, giúp chuyển đổi số và giám sát, đo lường hoạt động bảo đảm an toàn thông tin mạng, bao gồm: (1) Nền tảng Hỗ trợ quản lý bảo đảm an toàn hệ thống thông tin theo cấp độ (đã được Sở Thông tin và Truyền thông triển

khai tại Công văn số 712/STTTT-CĐSBCVT ngày 11/4/2024); (2) Nền tảng Hỗ trợ điều phối, ứng cứu sự cố; (3) Nền tảng Hỗ trợ điều tra số ((2) và (3) đã được Sở Thông tin và Truyền thông triển khai tại Công văn số 842/STTTT-VTCNTT ngày 09/5/2023).

- Sử dụng hiệu quả các nền tảng số khác khi được Sở Thông tin và Truyền thông hướng dẫn nhằm đảm bảo triển khai công tác bảo đảm an toàn thông tin thống nhất, đồng bộ và thuận lợi, hiệu quả hơn nữa.

5. Phòng chống lừa đảo trực tuyến

- Đảm bảo 100% người dân trên địa bàn tỉnh được tuyên truyền thường xuyên, liên tục thông qua các tổ chức mạng lưới, phương tiện thông tin đại chúng, hệ thống thông tin cơ sở, mạng xã hội,...

- Tham gia Liên minh Phòng chống lừa đảo trực tuyến trên không gian mạng do Bộ Thông tin và Truyền thông thành lập để hướng dẫn, kết nối, cung cấp thông tin, tài liệu và triển khai các giải pháp kỹ thuật phòng chống lừa đảo trực tuyến thông qua 04 hướng tiếp cận chính: (1) thông qua mạng viễn thông; (2) thông qua mạng xã hội; (3) thông qua tuyên truyền, giáo dục; (4) thông qua công nghệ.

- Triển khai các hoạt động theo hướng dẫn của Bộ Thông tin và Truyền thông và Liên minh. Liên hệ Cục An toàn thông tin hoặc truy cập Cổng không gian mạng quốc gia (khonggianmang.vn), website của Cục An toàn thông tin (ais.gov.vn) để kịp thời nhận được cảnh báo, cung cấp miễn phí nội dung tuyên truyền (video, tài liệu, poster, bài viết,...). Tận dụng tối đa tất cả các kênh tuyên truyền như: sự kiện, mạng xã hội, website, hệ thống thư điện tử, tin nhắn SMS, các ứng dụng thông minh,... để tuyên truyền thường xuyên, liên tục tới toàn thể cán bộ, công chức, viên chức, người lao động của cơ quan và người dân trên địa bàn thông qua các hệ thống thông tin cơ sở (đài truyền thanh, đài truyền hình), các Tổ công nghệ số cộng đồng để tuyên truyền nhận thức, kỹ năng cho người dân, nhất là ở vùng nông thôn, vùng xa. Khuyến nghị việc tuyên truyền qua các kênh nêu trên theo định kỳ hàng tuần, tháng, quý tùy theo nội dung để đảm bảo tính thường xuyên, liên tục.

- Phối hợp các cơ quan chức năng thường xuyên cập nhật thông tin, tiếp nhận cảnh báo từ Cục An toàn thông tin - Bộ Thông tin và Truyền thông, Sở Thông tin và Truyền thôn, Sở Y tế và các cơ quan có liên quan để kịp thời triển khai tuyên truyền tới người sử dụng khi có những vấn đề an toàn thông tin, hình thức tấn công mạng mới phát sinh.

- Tổ chức xây dựng một số nội dung tuyên truyền ấn tượng, phù hợp với đặc điểm, đặc trưng, bản sắc văn hóa của ngành, địa phương để tạo hiệu quả cao và phạm vi tuyên truyền rộng đến mọi đối tượng trong cộng đồng.

- Tham gia hưởng ứng mạnh mẽ Chiến dịch Tuyên truyền nâng cao nhận thức về an toàn thông tin do Bộ Thông tin và Truyền thông phát động.

6. Diễn tập thực chiến an toàn thông tin mạng

Bố trí, tạo điều kiện thuận lợi cho nhân sự là thành viên của Tổ chuyên trách An toàn thông tin và Đội Ứng cứu sự cố của tỉnh tham gia diễn tập theo Kế hoạch số 134/KH-UBND ngày 27/5/2024 của Ủy ban nhân dân tỉnh về tổ chức Diễn tập thực chiến an toàn thông tin, ứng cứu sự cố tỉnh Bà Rịa-Vũng Tàu năm 2024.

Đề nghị Thủ trưởng các đơn vị liên quan nghiêm túc tổ chức thực hiện các nội dung nêu trên./.

Nơi nhận :
- Như trên;
- Giám đốc SYT;
- Các Phó Giám đốc SYT;
- Website Sở Y tế;
- Lưu: VT, KHTC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Bùi Chí Tình