ỦY BAN NHÂN DÂN TỈNH BÀ RỊA - VŨNG TÀU	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 13 /KH-UBND	*Bà Rịa - Vũng Tàu, ngày 10 tháng 02 năm 2023*

KẾ HOẠCH

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"

Ngày 10/8/2022, Thủ tướng Chính phủ ban hành Quyết định số 964/QĐ-TTg về việc 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" (viết tắt là Quyết định số 964/QĐ-TTg).

Căn cứ chức năng, nhiệm vụ được phân công trong Quyết định số 964/QĐ-TTg, UBND tỉnh Bà Rịa - Vũng Tàu ban hành Kế hoạch triển khai thực hiện Quyết định số 964/QĐ-TTg trên địa bàn tỉnh, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Tăng cường hiệu lực quản lý nhà nước đối với bảo đảm an toàn, an ninh mạng; chủ động ứng phó với các thách thức từ không gian mạng; tổ chức quán triệt đầy đủ các mục tiêu, nhiệm vụ, giải pháp đề ra trong Quyết định số 964/QĐ-TTg.

- Chuyển đổi căn bản về nhận thức và cách làm để thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa an toàn, an ninh mạng (cyber resilience): Từ mô hình bảo vệ phân tán sang mô hình bảo vệ tập trung; từ bị động ứng cứu sự cố sang chủ động dự báo sớm, cảnh báo sớm, phòng ngừa và ứng phó hiệu quả; từ đơn độc bảo vệ, giấu kín thông tin bị tấn công mạng sang chủ động hợp tác, chia sẻ thông tin nhằm chủ động phòng ngừa và hỗ trợ xử lý sự cố, phục hồi hoạt động bình thường của hệ thống thông tin.

- Khởi tạo, duy trì môi trường mạng an toàn, lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và người dân; nắm bắt kịp thời, tận dụng hiệu quả các cơ hội do không gian mạng mang lại để phát triển kinh tế, xã hội, chủ động phòng ngừa, sẵn sàng ứng phó để hạn chế các tác động tiêu cực, bảo đảm quốc phòng, chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội và sự ổn định, phát triển của địa phương trong thời đại Cách mạng công nghiệp lần thứ tư.

2. Yêu cầu

- Phát huy sức mạnh của cả hệ thống chính trị và toàn xã hội nhằm xây dựng không gian mạng văn minh, lành mạnh, là động lực tham gia cuộc Cách mạng công nghiệp lần thứ tư. Năng lực về bảo đảm an toàn, an ninh mạng được nâng cao, chủ động, sẵn sàng ứng phó từ sớm, từ xa với các nguy cơ, thách thức, hoạt động gây

tổn hại tới chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng và an toàn thông tin mạng nhằm bảo vệ vững chắc chủ quyền, lợi ích quốc gia trên không gian mạng, quốc phòng, an ninh, trật tự an toàn xã hội và công cuộc chuyển đổi số, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng; trong đó cơ quan quản lý nhà nước giữ vai trò điều phối, gắn kết, chia sẻ thông tin.

- Xác định nguồn lực của chính quyền là cơ bản, quyết định; sự tham gia của các tổ chức, doanh nghiệp và phát huy sức mạnh quần chúng nhân dân là quan trọng, đột phá. Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông phối hợp chia sẻ thông tin giám sát không gian mạng nhằm phục vụ công tác bảo đảm an toàn, an ninh mạng và bảo vệ chủ quyền quốc gia trên không gian mạng.

II. NHIỆM VỤ TRỌNG TÂM

1. Tổ chức quán triệt, triển khai

Công an tỉnh chủ trì, phối hợp với Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông tổ chức tuyên truyền, phổ biến, quán triệt nội dung của Quyết định số 964/QĐ-TTg đến cán bộ, công chức, viên chức, lực lượng vũ trang và quần chúng nhân dân trên địa bàn tỉnh, đảm bảo phù hợp với chức năng, nhiệm vụ, thẩm quyền được giao. Nội dung tuyên truyền phải thể hiện đầy đủ nội dung trọng tâm của Quyết định số 964/QĐ-TTg và bám sát tinh thần chỉ đạo, nhiệm vụ trọng tâm tại các văn bản: Nghị quyết số 29-NQ/TW, ngày 25/5/2018 của Bộ Chính trị về "Chiến lược bảo vệ Tổ quốc trên không gian mạng"; Nghị quyết số 30-NQ/TW, ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia; Nghị quyết số 22/NQ-CP, ngày 18/10/2019 của Chính phủ về "Chương trình hành động thực hiện Nghị quyết số 30-NQ/TW, ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia"; Luật An toàn thông tin mạng; Luật An ninh mạng; Nghị định số 53/2022/NĐ-CP, ngày 15/8/2022 của Chính phủ về "Quy định chi tiết một số điều của Luật An ninh mạng".

2. Tăng cường vai trò quản lý của Nhà nước về an toàn, an ninh mạng

- Tiểu ban An toàn, An ninh mạng tỉnh điều phối chung sự phối hợp giữa 4 lực lượng (Công an, Quân sự, Thông tin và Truyền thông và Ban Tuyên giáo Tỉnh ủy), chủ động, phối hợp thực hiện theo chức năng, nhiệm vụ được giao để tham mưu UBND tỉnh tổ chức thực hiện các mặt công tác về an toàn, an ninh mạng.

- Sở Thông tin và Truyền thông chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan nghiên cứu, xây dựng cơ chế hợp tác giữa cơ quan nhà nước và các doanh nghiệp, hiệp hội doanh nghiệp trong xây dựng và thực thi các chính sách về an toàn, an ninh mạng; thường xuyên tuyên truyền, phổ biến chủ trương của Đảng, chính sách, pháp luật của Nhà nước về an toàn, an ninh mạng, kỹ năng tham gia trên không gian mạng an toàn, lành mạnh, hữu ích.

- Sở Khoa học và Công nghệ chủ trì, phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, đơn vị có liên quan nghiên cứu, tổ chức thực hiện các giải pháp chuyển giao và ứng dụng công nghệ, kỹ thuật an toàn, an ninh mạng; thúc đẩy, tạo môi trường thuận lợi và hỗ trợ có trọng tâm, trọng điểm để các tổ chức, cá nhân tham gia bảo vệ an toàn thông tin mạng và an ninh mạng.

- Thủ trưởng các cơ quan, đơn vị, lãnh đạo các địa phương trực tiếp chỉ đạo và chịu trách nhiệm về công tác bảo đảm an toàn, an ninh mạng, chủ động rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để tổ chức thực hiện có hiệu quả; phát huy sự tham gia tích cực, tự giác 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.

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

a) Các sở, ban, ngành, địa phương chủ trì, phối hợp với Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông tổ chức triển khai thực hiện các biện pháp bảo vệ chủ quyền quốc gia trên không gian mạng phù hợp với tình hình thực tế và chức năng, nhiệm vụ được giao của đơn vị, địa phương.

b) Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông:

- Xây dựng năng lực tự chủ, tham vấn các đơn vị chuyên trách về an toàn, an ninh mạng cấp trung ương để phản ứng, xử lý kịp thời, hiệu quả các hoạt động xâm phạm chủ quyền quốc gia trên không gian mạng của địa phương.

- Tham gia các diễn đàn, hội nghị, hội thảo về bảo vệ chủ quyền quốc gia trên không gian mạng do các cấp, các ngành tổ chức.

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 đặt trên địa bàn tỉnh

Công an tỉnh chủ trì, phối hợp với Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông, các cơ quan, đơn vị có liên quan tổ chức thực hiện các nhiệm vụ:

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

- Bảo đảm an toàn, an ninh mạng trong quá trình xây dựng, vận hành, khai thác cơ sở hạ tầng không gian mạng quốc gia của địa phương; giám sát, cảnh báo sớm các hành vi vi phạm pháp luật trên không gian mạng đối với cơ sở hạ tầng không gian mạng quốc gia trên địa bàn tỉnh.

- Nâng cao năng lực tự chủ về an toàn, an ninh mạng.

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

b) Bảo vệ hạ tầng số, nền tảng số

Công an tỉnh chủ trì, phối hợp với Sở Thông tin và Truyền thông, các cơ quan, đơn vị có liên quan tổ chức thực hiện các nhiệm vụ:

- Xây dựng Trung tâm điều hành an toàn thông tin mạng (SOC) tiếp nhận và phân tích dữ liệu nhằm dự báo, cảnh báo sớm các nguy cơ, rủi ro trên không gian mạng, các lỗ hổng bảo mật trên diện rộng, lộ lọt dữ liệu nghiêm trọng giúp các cơ quan, đơn vị, tổ chức, doanh nghiệp trên địa bàn tỉnh ngăn chặn kịp thời các cuộc tấn công mạng, giảm thiệt hại trên diện rộng.

- Xây dựng phương án bảo đảm an ninh chính trị nội bộ, an ninh kinh tế tại các sở, ban, ngành, địa phương có cơ sở hạ tầng không gian mạng, hạ tầng số, nền tảng quan trọng phục vụ chuyển đổi số, phát triển kinh tế số, xã hội số theo chức năng, nhiệm vụ được giao.

- Thường xuyên tiến hành rà quét, xử lý bóc gỡ mã độc trong hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh.

- Chủ động giám sát, phát hiện và công bố hành vi vi phạm pháp luật thuộc phạm vi quản lý trên các nền tảng số. Xử lý theo thẩm quyền hoặc tham mưu UBND tỉnh phối hợp với Bộ Công an, Bộ Thông tin và Truyền thông xử lý tổ chức, cá nhân vi phạm, gỡ bỏ thông tin vi phạm liên quan đến tỉnh BR-VT trên các nền tảng số.

- Hướng dẫn, kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ hạ tầng số, nền tảng số thực thi trách nhiệm bảo đảm an toàn thông tin mạng, bảo đảm an ninh mạng, bảo vệ chủ quyền quốc gia trên không gian mạng, phòng chống chiến tranh thông tin, chiến tranh không gian mạng theo chức năng, nhiệm vụ được giao.

c) Bảo vệ dữ liệu của tổ chức, cá nhân

Công an tỉnh chủ trì, phối hợp với Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông, các cơ quan, đơn vị có liên quan tổ chức thực hiện các nhiệm vụ:

- Bảo đảm an ninh mạng, an toàn thông tin mạng theo cấp độ hệ thống cơ sở dữ liệu của cơ quan, tổ chức, doanh nghiệp trên địa bàn tỉnh.

- Thường xuyên chia sẻ thông tin, tăng cường giám sát, thu thập, phân tích, nghiên cứu, phán đoán và cảnh báo sớm về nguy cơ trong bảo mật dữ liệu; xây dựng cơ chế phản ứng khẩn cấp trong trường hợp xảy ra sự cố bảo mật dữ liệu.

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

a) Chủ quản hệ thống thông tin

- 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.

- Chủ động rà soát, căn cứ hướng dẫn của Công an tỉnh, Sở Thông tin và Truyền thông nhằm lập hồ sơ đề nghị đưa hệ thống thông tin 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. Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng Make in Viet Nam.

- 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. Tối thiểu 01 năm/1 lần tổ chức diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn, an ninh mạng.

- Phối hợp với lực lượng chuyên trách về an ninh mạng của Công an tỉnh, Sở Thông tin và Truyền thông nhằm kết nối với Trung tâm An ninh mạng quốc gia để giám sát an ninh mạng.

b) Công an tỉnh

- Tổ chức kiểm tra, đánh giá an ninh mạng đối với các thiết bị kỹ thuật, phương tiện điện tử, phần mềm sử dụng trong những hệ thống thông tin quan trọng về an ninh quốc gia trước khi đưa vào sử dụng, nhất là những thiết bị, phương tiện được nước ngoài, doanh nghiệp tài trợ hoặc tặng, cho.

- Phối hợp, tham gia tư vấn, thẩm định về an ninh mạng đối với các hệ thống thông tin quan trọng về an ninh quốc gia.

- Chủ động xây dựng kế hoạch, tổ chức kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia và hệ thống thông tin khác của các cơ quan Đảng, Nhà nước theo kế hoạch hàng năm hoặc khi có đề nghị của chủ quản hệ thống thông tin.

- Chủ trì, phối hợp với Sở Thông tin và Truyền thông, Bộ Chỉ huy Quân sự tỉnh, các sở, ban, ngành, địa phương có liên quan xây dựng kế hoạch và tổ chức diễn tập thực chiến về an ninh mạng, xây dựng cơ chế phối hợp, chia sẻ thông tin giám sát an toàn, an ninh mạng hệ thống thông tin, có sự tham gia của các chủ quản hệ thống thông tin, cơ quan, tổ chức, doanh nghiệp bảo đảm an ninh mạng.

- Xây dựng mạng lưới ứng phó, khắc phục sự cố an ninh mạng của tỉnh, lấy lực lượng chuyên trách bảo vệ an ninh mạng làm trung tâm, phối hợp với các cơ quan, tổ chức, cá nhân trong quá trình ứng phó, khắc phục sự cố an ninh mạng.

- Phối hợp chủ quản hệ thống thông tin khắc phục, xử lý nguy cơ bị đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, phần mềm độc hại.

- Triển khai các biện pháp phòng ngừa, đấu tranh, xử lý hành vi xâm phạm an ninh mạng, hoạt động của các thế lực thù địch, các loại đối tượng sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.

c) Bộ Chỉ huy Quân sự tỉnh

- Chủ động, kịp thời phát hiện và ngăn chặn các nguy cơ mất an toàn, an ninh mạng nhằm bảo vệ chủ quyền quốc gia trên không gian mạng, phòng chống chiến tranh thông tin, chiến tranh không gian mạng.

- Tổ chức lực lượng bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quân sự theo chức năng, nhiệm vụ được giao.

- Đề xuất xây dựng các hệ thống kỹ thuật nghiệp vụ, triển khai các biện pháp phòng ngừa, đấu tranh với hoạt động của các thế lực thù địch sử dụng không gian mạng xâm phạm quốc phòng, chủ quyền quốc gia trên không gian mạng.

d) Sở Thông tin và Truyền thông

- Phát triển mạng lưới ứng cứu sự cố an toàn thông tin mạng nhằm phối hợp kịp thời, đồng bộ, hiệu quả giữa các lực lượng để bảo đảm an toàn thông tin mạng, tập trung vào 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng.

- Phát triển, chuyển giao các hệ thống kỹ thuật khác phục vụ bảo đảm an toàn thông tin mạng, bảo đảm an toàn thông tin cho quá trình chuyển đổi số, xây dựng Chính quyền số, kinh tế số, xã hội số.

đ) Công an tỉnh, Sở Thông tin và Truyền thông, Bộ Chỉ huy Quân sự tỉnh chủ động thực hiện giám sát, cảnh báo sớm để bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh theo chức năng, nhiệm vụ được giao, phòng tránh các nguy cơ mất an toàn, an ninh mạng, bị tấn công mạng, gián điệp mạng, chiến tranh mạng.

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

a) Chủ quản hệ thống 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.

- Đầu tư 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.

- Ít nhất 01 lần/năm tổ chức diễn tập, hướng dẫn, kiểm tra, ứng phó, ứng cứu sự cố an toàn thông tin cho các lĩnh vực quan trọng cần bảo đảm an toàn thông tin.

b) Các cơ quan chuyên trách an toàn, an ninh mạng (Bộ Chỉ huy Quân sự tỉnh, Công an tỉnh, Sở Thông tin và Truyền thông) tăng cường phối hợp chia sẻ thông tin về nguy cơ, rủi ro an toàn thông tin mạng cho chủ quản hệ thống thông tin quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng.

c) Công an tỉnh hướng dẫn, kiểm tra công tác bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin quan trọng thuộc phạm vi quản lý.

d) Bộ Chỉ huy Quân tỉnh sự hướng dẫn, kiểm tra công tác bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin quan trọng thuộc phạm vi quản lý.

đ) Sở Thông tin và Truyền thông hướng dẫn, kiểm tra công tác bảo đảm an toàn thông tin mạng và ứng cứu sự cố đối với các hệ thống thông tin quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (trừ các hệ thống thông tin thuộc phạm vi quản lý của Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh).

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

a) Công an tỉnh

- Thiết lập đường dây nóng, hệ thống tiếp nhận, xử lý thông tin về tội phạm mạng từ không gian mạng để quần chúng nhân dân phản ánh kịp thời, trực tiếp các hành vi vi phạm pháp luật trên không gian mạng tới cơ quan chức năng.

- Đổi mới nội dung, hình thức, biện pháp xây dựng phong trào toàn dân bảo vệ an ninh Tổ quốc phù hợp với thực tiễn chuyển đổi số. Phát huy vai trò của thế trận An ninh nhân dân trên không gian mạng để hình thành mô hình toàn dân bảo vệ an ninh Tổ quốc trên không gian mạng.

- Xây dựng cơ chế phối hợp với các sở, ban, ngành, địa phương, giữa lực lượng chuyên trách bảo vệ an ninh mạng với các tổ chức, doanh nghiệp có liên quan theo quy định pháp luật trong thực hiện công tác phòng ngừa, phát hiện, điều tra, xử lý các vi phạm pháp luật trên không gian mạng và phòng, chống khủng bố mạng.

- Gắn hoạch định, thực hiện chính sách phát triển kinh tế, xã hội với công tác phòng, chống tội phạm mạng. Tăng cường giáo dục, bồi dưỡng kiến thức quốc phòng, an ninh mạng.

b) Sở Thông tin và Truyền thông

- Thúc đẩy phát triển ứng dụng Internet an toàn nhằm bảo vệ người dân trên môi trường mạng.

- Phát triển ứng dụng tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin cho người sử dụng.

- Phát triển nền tảng hỗ trợ bảo vệ trẻ em trên môi trường mạng.

- Hướng dẫn tổ chức, cá nhân thay đổi thói quen, hành vi trên môi trường mạng theo các chuẩn mực an toàn.

- Đổi mới phương thức tuyên truyền, nâng cao nhận thức, phổ biến kiến thức và thay đổi thái độ của người dân về an toàn thông tin mạng với quan điểm lấy cộng đồng làm trung tâm, qua các hình thức như: ứng dụng trên điện thoại, mạng xã hội. Cung cấp cho tổ chức, cá nhân thông tin, cảnh báo, giải đáp thắc mắc về an toàn thông tin mạng; hỗ trợ tiện ích và hướng dẫn xử lý sự cố an toàn thông tin mạng.

- Thiết lập kênh trao đổi, làm việc nhằm khuyến khích, hỗ trợ và xây dựng cẩm nang hướng dẫn các tổ chức, doanh nghiệp (nhất là doanh nghiệp vừa và nhỏ) triển khai giải pháp bảo đảm an toàn thông tin mạng.

- Triển khai Chương trình Bảo vệ và hỗ trợ trẻ em tương tác lành mạnh, sáng tạo trên môi trường mạng giai đoạn 2021 - 2025.

- Hướng dẫn doanh nghiệp nền tảng số xây dựng và triển khai cơ chế để người dùng phản ánh, xử lý tin giả, tin không đúng sự thật.

c) Bộ Chỉ huy Quân sự tỉnh

- Nghiên cứu nội dung, hình thức xây dựng Thế trận Quốc phòng toàn dân trên không gian mạng gắn với Thế trận An ninh nhân dân trên không gian mạng.

- Tăng cường giám sát để kịp thời phát hiện, cảnh báo sớm các nguy cơ xâm phạm quốc phòng, chủ quyền quốc gia trên không gian mạng, góp phần xây dựng không gian mạng an toàn, lành mạnh.

- Phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung bí mật nhà nước trong phạm vi quản lý.

- Phối hợp với các sở, ban, ngành, địa phương thực hiện phòng ngừa, phát hiện, xử lý hành vi tấn công mạng, hành vi chống phá Đảng, Nhà nước; phòng, chống khủng bố mạng đối với các hệ thống thông tin trong phạm vi quản lý.

d) Các sở, ban, ngành, địa phương tăng cường phối hợp với các cơ quan chuyên trách an toàn, an ninh mạng của tỉnh (Công an tỉnh, Sở Thông tin và Truyền thông, Bộ Chỉ huy Quân sự tỉnh) trong hoạt động giám sát, phát hiện và phối hợp với các cơ quan, tổ chức có liên quan và các doanh nghiệp nền tảng số để xử lý tin giả, thông tin vi phạm pháp luật trong phạm vi quản lý; xây dựng và phát triển các website, trang mạng xã hội, tài khoản trên môi trường mạng uy tín, nhiều tương tác để phục vụ 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. Làm chủ, tự chủ công nghệ, sản phẩm, dịch vụ đủ khả năng chủ động ứng phó với các thách thức từ không gian mạng

a) Sở Thông tin và Truyền thông

- Nghiên cứu, phát triển và chuyển giao:

+ Hỗ trợ doanh nghiệp, cơ sở nghiên cứu có năng lực làm chủ và sáng tạo về giải pháp công nghệ để phát triển giải pháp an toàn thông tin mạng trọng điểm.

+ Thúc đẩy ý tưởng khởi nghiệp sáng tạo xuất sắc, phục vụ lợi ích quốc gia.

- Hợp tác công tư:

+ Định hướng, giao nhiệm vụ cho các doanh nghiệp giải quyết các vấn đề về an toàn thông tin mạng.

+ Thúc đẩy sứ mệnh của doanh nghiệp về bảo đảm an toàn thông tin mạng.

b) Công an tỉnh

- Kế thừa công nghệ, sản phẩm, dịch vụ an ninh mạng do Bộ Công an đầu tư, chuyển giao công nghệ; nghiên cứu, đề xuất UBND tỉnh đầu tư, ứng dụng.

- Từng bước tiếp cận, xác định lộ trình phù hợp về an ninh mạng, tiến tới từng bước làm chủ công nghệ nhằm giải quyết những nguy cơ, thách thức về an ninh mạng và phục vụ cho sự nghiệp phát triển kinh tế, xã hội của địa phương.

c) Bộ Chỉ huy Quân sự tỉnh

- Xây dựng hệ thống thông tin phục vụ nhiệm vụ quân sự, quốc phòng trên không gian mạng theo chức năng, nhiệm vụ được giao.

- Thúc đẩy các cơ quan, đơn vị, doanh nghiệp trực thuộc nghiên cứu, sản xuất sản phẩm, dịch vụ an toàn, an ninh mạng phù hợp với định hướng phát triển công nghiệp quốc phòng.

d) Sở Ngoại vụ

Phối hợp với Bộ Chỉ huy Quân sự tỉnh, Công an tỉnh, Sở Thông tin và Truyền thông trong hoạt động ký kết thỏa thuận hợp tác quốc tế về an toàn, an ninh mạng đối với một số tổ chức quốc tế có uy tín về an toàn, an ninh mạng.

9. Đào tạo và phát triển nguồn nhân lực

a) Sở Thông tin và Truyền thông

- 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.

- Phát triển đội ngũ chuyên gia xuất sắc về an toàn thông tin mạng; liên kết nguồn nhân lực an toàn thông tin trong các doanh nghiệp công nghệ số và doanh nghiệp an toàn thông tin mạng; hướng dẫn, thúc đẩy triển khai quy định chuẩn kỹ năng an toàn thông tin mạng.

- Tuyên dương, khen thưởng kịp thời đối với các cơ quan, tổ chức, doanh nghiệp, cá nhân có cống hiến cho an toàn thông tin mạng.

b) Công an tỉnh

- Tham mưu, đề xuất sử dụng kinh phí từ nguồn ngân sách địa phương để mời các chuyên gia về an ninh mạng tập huấn, thuê khoán chuyên gia giảng dạy, nghiên cứu, phát triển và tham gia các nhiệm vụ về an ninh mạng của địa phương.

- Chủ trì tham mưu triển khai Đề án "Đào tạo nguồn nhân lực an ninh mạng đến năm 2025, tầm nhìn đến năm 2030".

- Tuyên dương, khen thưởng kịp thời đối với các cơ quan, tổ chức, doanh nghiệp, cá nhân có cống hiến cho bảo đảm an ninh mạng.

c) Bộ Chỉ huy Quân sự tỉnh

- Chủ trì, phối hợp với các sở, ban, ngành, địa phương xây dựng và triển khai thực hiện có hiệu quả các chương trình đào tạo, phát triển nguồn nhân lực cho lực lượng tác chiến trên không gian mạng.

- Đầu tư xây dựng cơ sở vật chất, kỹ thuật phục vụ huấn luyện, bồi dưỡng nghiệp vụ và nghiên cứu khoa học về tác chiến trên không gian mạng.

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

a) Sở Thông tin và Truyền thông

- Triển khai Đề án "Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 - 2025".

- 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 đến người sử dụng Internet; triển khai trang bị kỹ năng cho các nhóm người yếu thế, dễ bị tổn thương trong xã hội hoạt động, tương tác trên môi trường không gian mạng.

- Phổ cập các sản phẩm, dịch vụ an toàn thông tin mạng cho người dùng.

- Xây dựng, hoàn thiện các kênh liên hệ, trao đổi để người dùng có thể thuận lợi phản ánh, chia sẻ và chung tay bảo đảm an toàn thông tin mạng.

b) Công an tỉnh

- Tổ chức các hoạt động tuyên truyền, nâng cao nhận thức, kiến thức về bảo đảm an ninh mạng hàng năm trên phạm vi cả tỉnh, với sự tham gia của các cơ quan truyền thông, báo chí, tổ chức, doanh nghiệp.

- Thiết lập các kênh, mạng xã hội để tuyên truyền, nâng cao nhận thức về bảo đảm an ninh mạng đối với quần chúng nhân dân về âm mưu, phương thức, thủ đoạn, các hành vi xâm phạm an ninh mạng, nâng cao sức đề kháng trước các thông tin xấu độc, thủ đoạn của các loại tội phạm sử dụng công nghệ cao.

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

Sở Thông tin và Truyền thông chủ trì, phối hợp với Sở Nội vụ, Sở Tài Chính, Sở Kế hoạch và Đầu tư nghiên cứu, tham mưu UBND tỉnh các nội dung:

a) Bố trí đủ nhân lực chuyên trách, chịu trách nhiệm về an toàn, an ninh mạng trong các cơ quan, tổ chức nhà nước; áp dụng các chính sách tài chính đặc thù nhằm hỗ trợ, bồi dưỡng cho lực lượng chuyên trách về an toàn thông tin mạng và an ninh mạng trong các cơ quan, tổ chức nhà nước.

b) 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. Ưu tiên bố trí nguồn lực để xây dựng các hệ thống kỹ thuật, công cụ bảo đảm an toàn, an ninh mạng có hiệu quả trong các cơ quan, tổ chức nhà nước.

III. TỔ CHỨC THỰC HIỆN

1. Căn cứ chức năng, nhiệm vụ và nội dung Kế hoạch này, Tiểu ban An toàn, An ninh mạng tỉnh, các sở, ban, ngành, UBND các huyện, thị xã, thành phố, cơ quan, đơn vị liên quan tổ chức quán triệt và triển khai thực hiện có hiệu quả các nhiệm vụ được giao.

2. Giao Tiểu ban An toàn, An ninh mạng tỉnh chủ trì hướng dẫn, kiểm tra, đôn đốc việc triển khai thực hiện Kế hoạch; tham mưu UBND tỉnh chỉ đạo, điều phối xử lý các vấn đề mới, quan trọng, liên ngành, chưa được quy định hoặc chồng chéo, phức tạp về an toàn, an ninh mạng; tổ chức sơ kết, tổng kết việc thực hiện Kế hoạch.

3. Trong quá trình triển khai thực hiện Kế hoạch, nếu có phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương kịp thời báo cáo UBND tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Công an tỉnh, bộ phận Thường trực Tổ giúp việc Tiểu ban An toàn, An ninh mạng tỉnh; đầu mối phối hợp: đồng chí Trung tá Đoàn Công Chính, Đội trưởng, số điện thoại 0936903878)* để được hướng dẫn, giải quyết./.

Nơi nhận:
- TTr Tỉnh ủy, TTr HĐND tỉnh;
- Cục A05 - Bộ Công an;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Các sở, ban, ngành;
- UBND các huyện, thị xã, thành phố;
- Lưu: VT, VPUB. (2)

CHỦ TỊCH

Nguyễn Văn Thọ