

Số: 395 /KH-UBND

Thừa Thiên Huế, ngày 05 tháng 12 năm 2023

KẾ HOẠCH

Triển khai thực hiện 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 trên địa bàn tỉnh Thừa Thiên Huế

Căn cứ 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 (sau đây gọi tắt là *Chiến lược*), UBND tỉnh ban hành Kế hoạch triển khai, thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU

- Thực hiện có hiệu quả Chiến lược; tạo sự chuyển biến mạnh mẽ về nhận thức, hành động của các cấp ủy Đảng, chính quyền các cấp và toàn thể đội ngũ cán bộ, công chức, viên chức, người lao động đối với việc thực hiện Chiến lược.

- Phát huy sức mạnh của cả hệ thống chính trị và toàn xã hội. Xác định nguồn lực nhà nước là quyết định, chiến lược, cơ bản lâu dài; sự tham gia của tổ chức, doanh nghiệp và phát huy sức mạnh của quần chúng nhân dân là quan trọng, đột phá.

- 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, lợi ích, quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, bảo vệ chủ quyền quốc gia trên không gian mạng và công cuộc chuyển đổi số quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

- Đẩy mạnh ứng dụng thành tựu khoa học - kỹ thuật, công nghệ tiên tiến, hiện đại thực hiện Chiến lược. Nghiên cứu các giải pháp xử lý, khắc phục lỗ hổng bảo mật, điểm yếu về bảo mật, an toàn thông tin.

- Xác định từng công việc cụ thể, phân công trách nhiệm rõ ràng, phù hợp với chức năng, nhiệm vụ của các Sở, ban, ngành, UBND các huyện, thành phố, thị xã và các cơ quan, đơn vị địa phương liên quan; thực thi tốt cơ chế phối hợp giữa các cơ quan, đơn vị trong quá trình thực hiện

II. NHIỆM VỤ VÀ GIẢI PHÁP

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

- 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, Mặt trận Tổ quốc, các tổ chức chính trị - xã hội, 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 thực hiện hiệu quả.

- Phát huy sự tham gia có hiệu quả 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.

- Hình thành Thế trận An ninh nhân dân trên không gian mạng kết hợp chặt chẽ với Thế trận Quốc phòng toàn dân trên không gian mạng.

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

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

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

- Công an Tỉnh, Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông và các sở, ban, ngành, địa phương, các cơ quan liên quan phối hợp bảo vệ chủ quyền quốc gia trên không gian mạng theo đúng chức năng, nhiệm vụ được giao.

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

a) Bảo vệ hạ tầng số:

- Sở Thông tin và Truyền thông:

+ Đôn đốc các doanh nghiệp cung cấp dịch vụ hạ tầng số trên địa bàn tỉnh có kế hoạch và phương án thực hiện công tác bảo đảm an toàn thông tin mạng trên hạ tầng số.

+ Chủ trì, phối hợp với các cơ quan chuyên môn, nghiệp vụ của Bộ Thông tin và Truyền thông 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, tổ chức, doanh nghiệp trên địa bàn tỉnh ngăn chặn kịp thời các cuộc tấn công mạng, giảm thiệt hại trên diện rộng.

+ Chủ trì xây dựng và trình cấp có thẩm quyền phê duyệt cấp độ an toàn thông tin, an ninh mạng đối với các hệ thống thông tin, cơ sở dữ liệu, nền tảng số do các sở, ban, ngành và địa phương quản lý và được cài đặt tại Trung tâm IOC và Cổng Thông tin điện tử tỉnh.

+ Tổ chức tốt các hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh và tham gia chiến dịch rà quét, xử lý bóc gỡ mã độc theo hướng dẫn, điều phối của Bộ Thông tin và Truyền thông.

- Bộ Chỉ huy Quân sự tỉnh:

+ Định kỳ kiểm tra an ninh, an toàn thông tin mạng của các đơn vị trực thuộc, các doanh nghiệp có hoạt động liên quan tới lĩnh vực quốc phòng trên địa bàn tỉnh.

+ Đôn đốc các doanh nghiệp hạ tầng số trên địa bàn tỉnh thực hiện trách nhiệm 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.

- Công an tỉnh:

+ Đôn đốc việc kiểm tra, đánh giá về an ninh mạng đối với hạ tầng mạng viễn thông.

b) Bảo vệ nền tảng số:

- Sở Thông tin và Truyền thông chủ trì, phối hợp với Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và các cơ quan liên quan chủ động kiểm tra, đánh giá các doanh nghiệp cung cấp dịch vụ nền tảng số trên địa bàn tỉnh thực hiện trách nhiệm bảo đảm an toàn thông tin mạng quốc gia theo chức năng, nhiệm vụ được giao.

- Bộ Chỉ huy quân sự tỉnh, Công an tỉnh chủ động kiểm tra, đánh giá các đơn vị trực thuộc, các doanh nghiệp trên địa bàn tỉnh có hoạt động liên quan đến lĩnh vực an ninh quốc phòng;

- Các Sở, ban, ngành, UBND cấp huyện, các đơn vị, tổ chức và doanh nghiệp:

+ Chủ động giám sát, phát hiện và báo cáo Chủ tịch UBND tỉnh các hành vi vi phạm quy định pháp luật của Việt Nam 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.

+ Tuyên truyền, hướng dẫn cán bộ, công chức, viên chức, người lao động và nhân dân lựa chọn sử dụng dịch vụ nền tảng số an toàn, lành mạnh.

+ Thận trọng khi cung cấp thông tin, dữ liệu cá nhân, đơn vị trên nền tảng số; bảo mật tài khoản, mật khẩu để không bị lộ lọt, lợi dụng thực hiện hành vi vi phạm pháp luật. Tuân thủ các quy tắc ứng xử, không đăng tải, lan truyền các nội dung vi phạm pháp luật trên môi trường mạng và chia sẻ, lan tỏa các thông tin tích cực; cảnh báo và phản ánh, tố giác các hành vi vi phạm pháp luật.

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

- Tuyên truyền chính sách, pháp luật về bảo vệ dữ liệu nhằm bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân, đặc biệt là dữ liệu quan trọng quốc gia và địa phương.

- Bảo đảm an ninh mạng, an toàn thông tin mạng theo cấp độ cho các cơ sở dữ liệu quốc gia và cơ sở dữ liệu quan trọng của các Sở, ban, ngành. Tăng cường thu thập, phân tích, nghiên cứu, phán đoán và cảnh báo sớm về thông tin rủi ro bảo mật dữ liệu.

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

- 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 (nếu cần thiết).

- 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 vận hành, 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 có xuất xứ Việt Nam (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.

- Định kỳ hàng năm tổ chức diễn tập nội bộ, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn, an ninh mạng.

- Định kỳ triển khai đánh giá an toàn thông tin cho các hệ thống thông tin đã được phê duyệt hồ sơ đề xuất cấp độ tương ứng.

- Triển khai cài đặt phần mềm phòng, chống mã độc tập trung cho các máy chủ; máy trạm của cán bộ, công chức, viên chức, người lao động trong cơ quan, đơn vị và chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

- Sử dụng các giải pháp dùng mật mã để bảo vệ hệ thống thông tin của đơn vị theo quy định.

b) Công an tỉnh

- Chủ động 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 trước khi đưa vào sử dụng, nhất là những thiết bị, phương tiện được nước ngoài, doanh nghiệp tài trợ, trao tặng.

- Xây dựng cơ chế phối hợp, tham gia tư vấn về an ninh mạng đối với các hệ thống thông tin quan trọng của tỉnh.

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

- Tham gia diễn tập thực chiến về an ninh mạng cấp quốc gia tổ chức. Xây dựng, hình thành Mạng lưới ứng phó, khắc phục sự cố an ninh mạng, lấy lực lượng chuyên trách bảo vệ an ninh mạng làm trung tâm, phối hợp chặt chẽ với các cơ quan, tổ chức, cá nhân trong ứng phó, khắc phục sự cố an ninh mạng.

- Phối hợp với cơ quan chuyên trách an ninh mạng của Bộ Công an chia sẻ thông tin giám sát an toàn, an ninh mạng.

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

- Triển khai các biện pháp phòng ngừa, đấu tranh, xử lý hành vi xâm phạm an ninh mạng, hoạt động của các đối tượng, thế lực thù địch 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 của cơ quan Đảng, Nhà nước. 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

- Tổ chức quản lý, vận hành hệ thống giám sát an toàn thông tin mạng tỉnh (SOC), thực hiện chia sẻ, dữ liệu về an toàn thông tin với Trung tâm Giám sát an toàn thông tin mạng quốc gia. Thực hiện giám sát các hệ thống thông tin quan trọng của tỉnh, kịp thời cảnh báo sớm, giúp ngăn chặn, xử lý kịp thời sự cố an toàn thông tin mạng.

- Chủ trì, phối hợp Công an tỉnh triển khai các giải pháp đảm bảo an toàn thông tin để duy trì kết nối, chia sẻ dữ liệu giữa Cơ sở dữ liệu quốc gia về dân cư và Hệ thống thông tin giải quyết thủ tục hành chính của tỉnh.

- Phối hợp với các đơn vị chức năng thuộc Bộ Thông tin và Truyền thông tổ chức đào tạo, sát hạch về an toàn thông tin trên nền tảng đào tạo, sát hạch trực tuyến kiến thức, kỹ năng an toàn thông tin cơ bản cho người sử dụng.

- Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia, mạng lưới ứng cứu sự cố an toàn thông tin mạng khu vực miền Trung và Tây Nguyên nhằm điều phối kịp thời, phối hợp đồng bộ, hiệu quả các lực lượng để bảo đảm an toàn thông tin mạng, tập trung vào các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng.

- Nghiên cứu, đề xuất các giải pháp kỹ thuật phục vụ bảo đảm an toàn thông tin mạng trên địa bàn tỉnh, bảo đảm an toàn thông tin cho quá trình chuyển đổi số, phát triển Chính quyền số, kinh tế số và xã hội số.

5. 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

- Xây dựng cơ chế, thiết lập đường dây nóng, hệ thống tiếp nhận, xử lý thông tin về tội phạm mạng từ không gian mạng để quản chúng nhân dân phản ánh kịp thời, trực tiếp thông tin, hành vi vi phạm pháp luật trên không gian mạng tới cơ quan chức năng có thẩm quyền.

- Đổi mới nội dung, hình thức, biện pháp xây dựng phong trào toàn dân bảo vệ an ninh Tổ quốc, hình thành mô hình toàn dân bảo vệ an ninh Tổ quốc trên không gian mạng.

- Xây dựng cơ chế phối hợp liên ngành trong tỉnh, phối hợp với Cục An toàn thông tin (Bộ Thông tin và Truyền thông), giữa lực lượng chuyên trách bảo vệ an ninh mạng với các tổ chức, doanh nghiệp có liên quan theo quy định của 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 chống khủng bố mạng.

b) Sở Thông tin và Truyền thông

- Tuyên truyền sử dụng việc sử dụng các ứng dụng (App) phổ biến kiến thức, nhận thức về an toàn thông tin cho người sử dụng và sử dụng Nền tảng hỗ trợ bảo vệ trẻ em trên môi trường mạng.

- 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 với quan điểm lấy cộng đồng làm trung tâm qua các hình thức như: ứng dụng trên điện thoại, mạng xã hội, nền tảng số Hue-S. Cung cấp cho tổ chức, cá nhân thông tin, cảnh báo, giải đáp thắc mắc về an toàn thông tin mạng tại địa chỉ <https://khonggianmang.vn>; hỗ trợ công cụ, 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 cảm 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.

- Chỉ đạo doanh nghiệp nền tảng số trên địa bàn tỉnh xây dựng và triển khai cơ chế để người sử dụng phản ánh, xử lý tin giả, thông tin không đúng sự thực về đất nước, con người Việt Nam và tỉnh Thừa Thiên Huế.

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.

- Kịp thời 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, đoàn thể, 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 và địa phương

- 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 và tỉnh Thừa Thiên Huế.

6. Đào tạo và phát triển nguồn nhân lực

a) Sở Thông tin và Truyền thông

- Triển khai các nội dung, nhiệm vụ của Đề án “Đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021 - 2025” tại Kế hoạch số 95/KH-UBND ngày 17/3/2021 của UBND tỉnh; nghiên cứu, đề xuất phương án thúc đẩy hoạt động trong lĩnh vực này giai đoạn 2026 - 2030.

- Phát triển đội ngũ chuyên gia giỏi về an toàn thông tin mạng. Phát triển và liên kết nguồn nhân lực an toàn thông tin trong các doanh nghiệp công nghệ số và doanh nghiệp an toàn thông tin mạng.

- Tham mưu UBND tỉnh 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 quốc gia.

b) Công an tỉnh

- Tham mưu UBND tỉnh xây dựng cơ chế, chính sách, pháp luật về đào tạo nguồn nhân lực về bảo đảm an ninh mạng.

- Xây dựng đội ngũ chuyên trách về an ninh mạng, đội ngũ kỹ sư an ninh mạng chất lượng cao. Ưu tiên đào tạo các tài năng trẻ, tạo điều kiện để các tài năng trẻ được học tập, nghiên cứu và phát triển.

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

c) Bộ Chỉ huy Quân sự tỉnh

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

- Tham mưu, đề xuất cơ sở vật chất, kỹ thuật phục vụ huấn luyện, bồi dưỡng nghiệp vụ và nghiên cứu khoa học về tác chiến không gian mạng; nghiên cứu, xây dựng chế độ, chính sách cho lực lượng tác chiến không gian mạng và các lực lượng tham gia bảo vệ Tổ quốc trên không gian mạng.

7. 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 các nội dung, nhiệm vụ của Kế hoạch số 47/KH-UBND ngày 18/02/2021 của UBND tỉnh về tuyên truyền nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021 – 2025 trên địa bàn tỉnh Thừa Thiên Huế; nghiên cứu, đề xuất phương án thúc đẩy hoạt động trong lĩnh vực này giai đoạn 2026 - 2030.

- 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.

- Thực hiện phổ cập các sản phẩm, dịch vụ an toàn thông tin mạng cơ bản cho người sử dụng.

- Thiết lập các kênh liên hệ, trao đổi trên nền tảng số Hue-S để người sử dụng có thể thuận lợi phản ánh, chia sẻ và chung tay bảo đảm an toàn thông tin mạng quốc gia.

- Phối hợp với các đơn vị chức năng thuộc Bộ Thông tin và Truyền thông triển khai các khóa học trực tuyến mở (MOOC) tuyên truyền, phổ biến kỹ năng an toàn thông tin cơ bản cho người dùng.

b) Công an tỉnh:

- Tổ chức các chiến dịch tuyên truyền, nâng cao nhận thức, kiến thức về bảo đảm an ninh mạng hàng năm.

- 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.

c) Cơ quan, tổ chức, doanh nghiệp, cơ sở giáo dục, đào tạo trên địa bàn tỉnh:

- 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.

- 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.

- Các cơ sở giáo dục, đào tạo xây dựng chương trình, kế hoạch học tập, rèn luyện kỹ năng cho học sinh, sinh viên về an toàn, an ninh mạng đối với các thông tin sai lệch trên không gian mạng.

- Các doanh nghiệp cung cấp dịch vụ số trên địa bàn tỉnh thực hiện tuyên truyền, nâng cao nhận thức, phổ biến kiến thức về an toàn, an ninh mạng; có biện pháp kỹ thuật hạn chế tin giả, tin sai sự thật, xấu, độc trên nền tảng, dịch vụ của mình.

- Các tổ chức truyền thông, cơ quan báo chí tăng cường thông tin về xu hướng, kiến thức, tình hình, nguy cơ, hậu quả an toàn, an ninh mạng thế giới và Việt Nam.

8. 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, tổ chức nhà nước. 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, tổ chức.

- Triển khai, hỗ trợ cơ chế tiền lương đặc thù cho lực lượng chuyên trách về an toàn thông tin mạng và an ninh mạng trong các cơ quan, tổ chức nhà nước theo quy định, hướng dẫn của trung ương.

- Ngân sách tỉnh bảo đảm kinh phí thực hiện các nhiệm vụ thuộc Chương trình, Kế hoạch do các Sở, ban, ngành, đoàn thể và địa phương thực hiện.

III. TỔ CHỨC THỰC HIỆN

1. Ban Chỉ đạo Chuyển đổi số tỉnh

Ban Chỉ đạo Chuyển đổi số tỉnh (Sở Thông tin và Truyền thông làm cơ quan Thường trực) giúp Chủ tịch UBND tỉnh chỉ đạo công tác sơ kết, tổng kết việc triển khai thực hiện; chỉ đạo, điều phối xử lý các vấn đề về an toàn, an ninh mạng thuộc nội dung Kế hoạch này.

2. Sở Thông tin và Truyền thông, Công an tỉnh

- Sở Thông tin và Truyền thông chủ trì, phối hợp với Công an tỉnh hướng dẫn, đôn đốc, kiểm tra các cơ quan, tổ chức, doanh nghiệp trên địa bàn tỉnh triển khai thực hiện các nội dung về an ninh mạng tại Kế hoạch này.

- Tổ chức sơ kết, tổng kết, tổng hợp, báo cáo Chủ tịch UBND tỉnh tình hình thực hiện và đề xuất, kiến nghị nhiệm vụ mới cho phù hợp với tình hình thực tiễn đối với các nội dung về an ninh mạng.

- Chủ trì, phối hợp với các sở, ban, ngành, huyện, thị xã, thành phố và tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ được giao tại phần II theo chức năng, nhiệm vụ.

3. Bộ Chỉ huy Quân sự tỉnh

- Thực hiện công tác phòng ngừa, ứng phó, xử lý các nguy cơ, thách thức từ không gian mạng, dự báo các tình huống về chiến tranh thông tin, xung đột trên không gian mạng theo chức năng, nhiệm vụ được giao.

- Chủ trì, phối hợp với các sở, ban, ngành, địa phương và tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ đã được giao tại phần II theo chức năng, nhiệm vụ.

4. Sở Khoa học và Công nghệ

- Chủ trì, phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, tổ chức, doanh nghiệp liên quan nghiên cứu, thực hiện chuyển giao công nghệ và tuyên truyền, phổ biến, hướng dẫn áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng.

- Chủ trì, phối hợp với các cơ quan liên quan triển khai hỗ trợ các nhiệm vụ khoa học và công nghệ liên quan đến an toàn thông tin và an ninh mạng để triển khai áp dụng trên địa bàn tỉnh

5. Sở Nội vụ

Chủ trì, phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông, Sở Tài chính nghiên cứu, tham mưu UBND tỉnh hỗ trợ cơ chế tiền lương đặc thù cho lực lượng chuyên trách về an toàn thông tin mạng và an ninh mạng trong các cơ quan, tổ chức nhà nước theo hướng dẫn của Trung ương.

6. Sở Tài chính

Căn cứ khả năng cân đối ngân sách, Sở Tài chính tham mưu UBND tỉnh bố trí kinh phí cho các nội dung chi thường xuyên đối với công tác đảm bảo an toàn thông tin và an ninh mạng trong các cơ quan nhà nước theo quy định của Luật ngân sách nhà nước và các văn bản hướng dẫn thi hành.

7. Sở Kế hoạch và Đầu tư

Nghiên cứu và tham mưu UBND tỉnh ưu tiên các nhiệm vụ về an toàn thông tin và an ninh mạng trong các dự án đầu tư theo quy định của pháp luật về đầu tư công.

8. Các sở, ban, ngành và UBND các huyện, thị xã và thành phố

- Chủ trì, phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông tổ chức thực hiện các nhiệm vụ được giao tại Kế hoạch này.

- Đẩy mạnh hoạt động bảo đảm an toàn, an ninh mạng trong phạm vi quản lý, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ theo quy định của pháp luật.

- Ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng, an ninh mạng do Việt Nam sản xuất (Makein Vietnam), gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác triển khai Chuyển đổi số, phát triển chính quyền số, gắn với đô thị thông minh và kinh tế số, xã hội số.

- Chủ động rà soát, phát hiện và xử lý hoặc phối hợp với các cơ quan chức năng có thẩm quyền xử lý thông tin vi phạm pháp luật trên môi trường mạng thuộc phạm vi quản lý. Tăng cường hoạt động thanh tra, kiểm tra, công bố và xử lý hoặc phối hợp xử lý nghiêm các hành vi vi phạm.

- Ưu tiên bố trí nguồn lực về nhân lực và kinh phí, cùng các điều kiện khác để triển khai hoạt động bảo đảm an toàn, an ninh mạng trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý.

- Thúc đẩy việc ứng dụng, sử dụng chữ ký số chuyên dùng Chính phủ và bảo mật thông tin trên hệ thống mạng theo quy định của pháp luật về cơ yếu.

- Định kỳ kiểm tra, đánh giá và báo cáo hàng năm hoặc đột xuất theo quy định do Công an tỉnh, Sở Thông tin và Truyền thông hướng dẫn về tình hình, kết quả triển khai Kế hoạch để tổng hợp, báo cáo Thủ tướng Chính phủ theo quy định về chế độ thông tin, báo cáo.

9. Các đơn vị truyền thông, cơ quan báo chí địa phương

- Sản xuất các tin, bài, phóng sự, câu chuyện cảnh giác, phim tài liệu về an toàn thông tin và an ninh mạng trên báo chí và phát thanh, truyền hình.

- Tìm kiếm, phổ biến kinh nghiệm, vụ việc về lừa đảo, tin giả, đánh cắp thông tin, tài khoản cá nhân, gây lộ lọt thông tin và ảnh hưởng đến an toàn, an ninh mạng trên các chuyên trang, chuyên mục tuyên truyền và trên các kênh có đông khán thính giả.

10. Hiệp hội Doanh nghiệp, Hội Công nghệ thông tin và Điện tử viễn thông, các công ty, doanh nghiệp nhà nước trên địa bàn tỉnh

Căn cứ nội dung của Kế hoạch này, tổ chức triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động của doanh nghiệp theo hướng dẫn của Công an tỉnh, và Sở Thông tin và Truyền thông.

11. Các doanh nghiệp viễn thông, Internet, nền tảng số trên địa bàn tỉnh

- Chủ động tích cực phối hợp triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động của doanh nghiệp.

- Tuân thủ các hướng dẫn, yêu cầu của Công an tỉnh, Sở Thông tin và Truyền thông trong hoạt động phát triển hạ tầng số, nền tảng số và bảo vệ dữ liệu số.

- Định kỳ hàng năm hoặc đột xuất báo cáo Công an tỉnh, Sở Thông tin và Truyền thông tình hình, kết quả triển khai các nhiệm vụ theo hướng dẫn.

Trên đây là kế hoạch Triển khai thực hiện 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 trên địa bàn tỉnh Thừa Thiên Huế (*Kế hoạch này thay thế cho Kế hoạch số 230/KH-UBND ngày 16/6/2023 của UBND tỉnh về Triển khai thực hiện 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 trên địa bàn tỉnh Thừa Thiên Huế*). UBND tỉnh yêu cầu các cơ quan, đơn vị, địa phương và tổ chức, doanh nghiệp nghiêm túc triển khai Kế hoạch này. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, đề nghị kịp thời phản ánh về Sở Thông tin và Truyền thông để báo cáo UBND tỉnh theo quy định./.

Nơi nhận:

- Bộ Công an;
- Bộ Thông tin và Truyền thông;
- Bộ Quốc phòng;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Chủ tịch và các Phó Chủ tịch;
- Văn phòng và các Ban Đảng thuộc Tỉnh ủy;
- Như mục III;
- VP: CVP, các PCVP;
- Lưu: VP, CN.



Nguyễn Văn Phương