ỦY BAN NHÂN DÂN TỈNH ĐẮK LẮK	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 37 /KH-UBND	*Đắk Lắk, ngày08 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

Triển khai Quyết định số 964/QĐ-TTg ngày 10/8/2022 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 *(sau đây viết tắt là Quyết định số 964/QĐ-TTg)*, Ủy ban nhân dân tỉnh ban hành Kế hoạch thực hiện với các nội dung 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 góp phần từng bước đưa công nghệ thông tin của tỉnh Đắk Lắk 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 trên địa bàn, 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, công cuộc chuyển đổi số, lĩnh vực quốc phòng, an ninh, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

2. Mục tiêu cụ thể đến năm 2025

a) Góp phần duy trì thứ hạng của Việt Nam từ 25 đến 30 về Chỉ số an toàn, an ninh mạng toàn cầu theo đánh giá của Liên minh Viễn thông quốc tế *(Chỉ số GCI)*.

b) Xây dựng được mạng lưới kết nối thông tin trên không gian mạng giữa các sở, ban, ngành, các doanh nghiệp viễn thông, Internet nhằm chia sẻ, tiếp nhận và xử lý sớm thông tin xấu độc trên mạng xã hội tại địa bàn.

c) Hình thành lực lượng chuyên trách tại các sở, ban, ngành, tổ chức chính

trị - xã hội, doanh nghiệp nhà nước và các doanh nghiệp khác trên địa bàn tỉnh có trách nhiệm trong công tác đảm bảo an toàn, an ninh mạng.

d) Các sở, ban, ngành, đơn vị thuộc Ủy ban nhân dân tỉnh, các tổ chức chính trị - xã hội, doanh nghiệp nhà nước, hiệp hội doanh nghiệp trên địa bàn nghiêm túc thực hiện tốt các quy định của pháp luật về bảo đảm thông tin và an ninh mạng.

đ) Bảo vệ cơ sở hạ tầng không gian mạng quốc gia, trọng tâm là hệ thống thông tin quan trọng về an ninh quốc gia theo quy định của pháp luật về an ninh mạng. Bảo vệ hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng trên địa bàn (theo Quyết định số 632/QĐ-TTg ngày 10 tháng 5 năm 2017 của Thủ tướng Chính phủ).

e) Phấn đấu 80% người sử dụng Internet trên địa bàn tỉnh có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

g) Chủ động tham mưu, đề xuất với Đảng, Nhà nước, Chính phủ 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.

h) Khuyến kích, thúc đẩy các doanh nghiệp trên địa bàn tham gia, phát triển các sản phẩm, dịch vụ có sự cạnh tranh về lĩnh vực an toàn thông tin, an ninh mạng nhằm góp phần tăng doanh thu (từ 10 đến 20%), phát triển kinh tế - xã hội tại địa phương.

i) Tham mưu, đề xuất với Đảng, Nhà nước bổ sung nguồn kinh phí bảo đảm an toàn, an ninh mạng phục vụ cho việc nghiên cứu khoa học công nghệ, viễn thông tin học, ứng dụng chuyển đổi số trên địa bàn.

3. Mục tiêu cụ thể đến năm 2030

a) Duy trì, góp phần nâng cao năng lực thứ hạng về Chỉ số an toàn, an ninh mạng của tỉnh, của Việt Nam trên bảng xếp hạng toàn cầu.

b) 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.

c) 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.

d) Phấn đấu 90% người sử dụng Internet trên địa bàn tỉnh có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng xử lý các tình huống trên không gian mạng.

đ) Thu hút các nhà khoa học, nhân tài về lĩnh vực công nghệ thông tin

nhằm từng bước hình thành các trung tâm nghiên cứu, phát triển, sáng tạo về an ninh mạng trên địa bàn, góp phần đưa Việt Nam trở thành một trong những trung tâm bảo đảm an toàn, an ninh mạng trong khu vực, châu Á.

II. NHIỆM VỤ, GIẢI PHÁP

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

a) 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, trong đó Tiểu ban An toàn, An ninh mạng tỉnh điều phối chung sự phối hợp giữa 4 lực lượng (Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông và Ban Tuyên giáo Tỉnh ủy). Các lực lượng này chủ động, phối hợp thực hiện theo chức năng, nhiệm vụ được giao.

b) 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.

c) 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 triển khai thực hiện các nhiệm vụ đạt hiệu quả.

d) 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.

đ) 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.

e) Ủy ban nhân dân tỉnh ưu tiên việc chuyển giao các ứng dụng công nghệ, kỹ thuật an toàn, an ninh mạng; thúc đẩy nghiên cứu, tạo môi trường thuận lợi và hỗ trợ có trọng tâm, trọng điểm để tổ chức, cá nhân tham gia vào công tác bảo đảm an toàn thông tin, an ninh mạng. Xây dựng cơ chế hợp tác giữa chính quyền địa phương với các doanh nghiệp, hiệp hội doanh nghiệp trên địa bàn trong việc triển khai các chủ trương, chính sách về an toàn, an ninh mạng. Đẩy mạnh công tác tuyên truyền, phổ biến kỹ năng tham gia không gian mạng an toàn.

2. Hoàn thiện hành lang pháp lý

a) Công an tỉnh

- Tham gia đề xuất xây dựng, hoàn thiện chính sách, pháp luật về bảo vệ an ninh mạng đồng bộ, thống nhất từ trung ương đến địa phương theo định hướng

điều chỉnh đầy đủ các lĩnh vực phát sinh hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội; nâng cao năng lực bảo vệ chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ được giao.

- Tham gia đề xuất xây dựng, hoàn thiện chính sách, pháp luật về bảo vệ dữ liệu quốc gia, dữ liệu cá nhân, quy định về hoạt động thu thập, lưu trữ, xử lý dữ liệu công dân Việt Nam và trách nhiệm của các tổ chức, doanh nghiệp trong và ngoài nước trong bảo vệ chủ quyền, an ninh quốc gia của Việt Nam trên không gian mạng.

- Tham gia góp ý sửa đổi, bổ sung các văn bản quy phạm pháp luật về an ninh mạng để đồng bộ, thống nhất, toàn diện, đáp ứng được yêu cầu đấu tranh, xử lý vi phạm pháp luật về an ninh mạng.

- Nghiên cứu, rà soát, đề xuất sửa đổi, bổ sung, hoàn thiện các văn bản hướng dẫn thi hành Luật An ninh mạng, các văn bản quy phạm pháp luật về điều kiện kinh doanh các sản phẩm, dịch vụ an ninh mạng, nhất là các sản phẩm, dịch vụ sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin của cơ quan nhà nước.

- Căn cứ các quy định của Nhà nước, phối hợp với Sở Thông tin và Truyền thông, Sở Khoa học và Công nghệ trong việc áp dụng cơ chế khoán chi cho các đề tài khoa học về an toàn, an ninh mạng.

b) Sở Thông tin và Truyền thông

- Tham gia xây dựng, hoàn thiện chính sách, pháp luật về an toàn thông tin mạng, nhất là các chế tài xử lý vi phạm pháp luật về an toàn thông tin mạng.

- Nghiên cứu, rà soát, tham gia đề xuất xây dựng, sửa đổi, bổ sung văn bản quy phạm pháp luật và văn bản hướng dẫn thi hành về bảo đảm an toàn thông tin mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, dữ liệu số, bảo vệ thông tin cá nhân trên mạng.

c) Bộ Chỉ huy Quân sự tỉnh

Tham gia xây dựng, hoàn thiện chính sách, pháp luật về lĩnh vực quốc phòng, bảo vệ Tổ quốc trên không gian mạng, bảo vệ chủ quyền quốc gia trên không gian mạng theo chức năng, nhiệm vụ được giao.

d) Các sở, ngành liên quan theo chức năng, nhiệm vụ được giao tổ chức bảo vệ đội ngũ chuyên gia, trí thức, nhân sự có trình độ, lĩnh vực 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

a) Nghiên cứu, đề xuất ban hành chủ trương, chính sách, pháp luật 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 các sở, ban, ngành có liên quan.

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

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

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 quốc gia trên địa bàn; 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 quốc gia trên địa bàn. 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.

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

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

- Đánh giá rủi ro an ninh mạng và xếp hạng năng lực bảo đảm an ninh mạng cấp tỉnh đối với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia theo tiêu chí đặt ra.

b) Bảo vệ hạ tầng số

- Sở Thông tin và Truyền thông:

+ Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp hạ tầng số *(cơ sở hạ tầng kỹ thuật số)*[1] trong việc triển khai, thực hiện công tác bảo đảm an toàn thông tin mạng quốc gia, an toàn thông tin mạng trên địa bàn theo chức năng, nhiệm vụ được giao.

+ Theo chức năng, nhiệm vụ được giao, thực hiện thu thập, tổng hợp, phân

[1] Các doanh nghiệp cung cấp hạ tầng viễn thông băng rộng, hạ tầng điện toán đám mây, hạ tầng internet kết nối vạn vật, hạ tầng cung cấp công nghệ như dịch vụ…trên địa bàn tỉnh như: Viettel Đắk Lắk, VNPT Đắk Lắk, FPT Đắk Lắk,…

tích dữ liệu lưu lượng truy cập Internet trên môi trường mạng trên địa bàn nhằm phát hiện các dấu hiệu, nguy cơ để dự báo sớm, kịp thời ngăn chặn hành vi tấn công mạng.

+ Chủ động phối hợp với các sở, ngành liên quan tổ chức rà quét, xử lý bóc gỡ mã độc trên địa bàn.

- Bộ Chỉ huy Quân sự tỉnh:

+ Chủ động chỉ đạo, kiểm tra các đơn vị trực thuộc và kịp thời trao đổi, phối hợp với các doanh nghiệp cung cấp viễn thông trên địa bàn liên quan đến hoạt động bảo đảm an toàn, an ninh mạng thuộc lĩnh vực quốc phòng.

+ Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp hạ tầng số trên địa bàn thực thi trách nhiệm và sứ mệnh 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.

+ Phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các sở, ngành liên quan trong công tác chỉ đạo, kiểm tra, đánh giá các doanh nghiệp trên địa bàn cung cấp dịch vụ nền tảng số thực thi trách nhiệm trong công tác bảo đảm an toàn, an ninh mạng.

- Công an tỉnh: Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp hạ tầng số trên địa bàn thực thi trách nhiệm và sứ mệnh bảo đảm an ninh mạng theo chức năng, nhiệm vụ được giao.

- Doanh nghiệp hạ tầng số *(cơ sở hạ tầng kỹ thuật số)*:

+ Cung cấp dịch vụ viễn thông, Internet an toàn (Security by Default).

+ Bảo đảm an toàn thông tin mạng 5G và các thế hệ mạng tiếp theo trong toàn bộ quá trình thiết kế, xây dựng và vận hành, khai thác, bao gồm:

Kiểm tra, đánh giá an toàn thông tin mạng (Pentest) và săn lùng mối nguy hại (Threat hunting). Xây dựng môi trường thử nghiệm (Test-bed) để diễn tập, nâng cao kỹ năng và tri thức cho chuyên gia an toàn thông tin của doanh nghiệp.

Kiểm tra, đánh giá an toàn thông tin mạng đối với các thiết bị đầu cuối trước khi cung cấp cho người sử dụng. Ưu tiên sử dụng các thiết bị đầu cuối do doanh nghiệp trong nước sản xuất đã được kiểm tra, đánh giá, công bố về an toàn thông tin mạng theo quy định.

+ Khắc phục, xử lý hoặc thay thế thiết bị đầu cuối cung cấp cho người sử dụng (Modem, Router, Camera giám sát, các thiết bị IoT,...) có dấu hiệu mất an toàn thông tin mạng.

+ Triển khai các ứng dụng điều hành, giám sát an toàn thông tin mạng

(SOC) trên địa bàn.

+ Phát triển hạ tầng mạng IoT an toàn, bao gồm:

Đánh giá, công bố đáp ứng tiêu chí kỹ thuật về an toàn thông tin đối với thiết bị IoT. Lựa chọn thiết bị IoT đã được đánh giá, công bố đáp ứng tiêu chí kỹ thuật về an toàn thông tin khi thiết lập hạ tầng mạng IoT.

Phát triển các sản phẩm, giải pháp cổng kết nối thiết bị IoT (IoT Gateway) "Make in Viet Nam" bảo đảm an toàn thông tin cho thiết bị IoT.

+ Bảo đảm an toàn thông tin mạng cho hạ tầng điện toán đám mây trên địa bàn, bao gồm: Phát triển hạ tầng điện toán đám mây "Make in Viet Nam"; kết nối các nền tảng cung cấp dịch vụ điện toán đám mây của Việt Nam (Multi Cloud), bảo đảm tính liên thông, an toàn, hiệu quả.

+ Công khai mức độ an toàn thông tin mạng của các dịch vụ hạ tầng số.

+ Ưu tiên sử dụng sản phẩm an toàn, an ninh mạng "Make in Viet Nam".

- Tổ chức, cá nhân sử dụng dịch vụ:

+ 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 xảy ra 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

- Doanh nghiệp chủ quản nền tảng số [2]:

+ Xác định cấp độ an toàn thông tin và triển khai phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đối với nền tảng số.

+ Phát triển nền tảng số có khả năng tự bảo vệ; có các công cụ sàng lọc, phát hiện, xử lý, gỡ bỏ thông tin vi phạm pháp luật trên nền tảng số.

+ Công khai chính sách quản lý, sử dụng thông tin, dữ liệu của người sử dụng trên nền tảng số. Bảo đảm an toàn thông tin cá nhân, thông tin về tài khoản, mật khẩu tin nhắn, lịch sử giao dịch của người sử dụng dịch vụ nền tảng số.

+ Cung cấp cho người sử dụng cơ chế khiếu nại, phản ánh, xác minh tin

[2] Bao gồm cơ quan nhà nước chủ quản, doanh nghiệp Việt Nam phát triển, làm chủ công nghệ lõi, sử dụng thống nhất trên toàn quốc, phục vụ hoạt động quản lý nhà nước hoặc cung cấp dịch vụ công phục vụ xã hội theo "Danh mục các nền tảng số quốc gia phục vụ chuyển đổi số, chính phủ số, kinh tế số, xã hội số" (Ban hành kèm theo Quyết định số 186/QĐ-BTTTT ngày 11/02/2022 của Bộ Thông tin và Truyền thông)

giả, thông tin vi phạm pháp luật và tiến hành xử lý theo quy định.

+ Chủ động phát hiện, ngăn chặn, xử lý, xóa bỏ tin giả, thông tin vi phạm pháp luật hoặc cung cấp các bằng chứng để truy vết, xác định nguồn gốc thông tin; xử lý, xóa bỏ thông tin vi phạm pháp luật theo yêu cầu của cơ quan chức năng có thẩm quyền.

+ Không cung cấp hoặc ngừng cung cấp dịch vụ cho tổ chức, cá nhân đăng tải trên môi trường mạng thông tin có nội dung vi phạm pháp luật Việt Nam.

+ Phát triển các nền tảng số "Make in Viet Nam" có hàng triệu người Việt Nam và quốc tế sử dụng.

- Sở Thông tin và Truyền thông: Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp trên địa bàn cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an toàn thông tin mạng quốc gia theo chức năng, nhiệm vụ được giao.

- Công an tỉnh: Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp trên địa bàn cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an ninh mạng theo chức năng, nhiệm vụ được giao.

- Bộ Chỉ huy Quân sự tỉnh:

+ Chủ động chỉ đạo, kiểm tra các đơn vị trực thuộc, các doanh nghiệp trên địa bàn có hoạt động liên quan tới lĩnh vực quốc phòng.

+ Chỉ đạo, kiểm tra, đánh giá các doanh nghiệp trên địa bàn cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh 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.

+ Phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan liên quan trong công tác chỉ đạo, kiểm tra, đánh giá các doanh nghiệp trên địa bàn cung cấp dịch vụ nền tảng số thực thi trách nhiệm và sứ mệnh bảo đảm an toàn, an ninh mạng.

- Các sở, ngành, địa phương: 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.

- Tổ chức, cá nhân sử dụng dịch vụ:

+ Lựa chọn sử dụng dịch vụ nền tảng số an toàn, lành mạnh.

+ Thận trọng khi cung cấp thông tin, dữ liệu cá nhân 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.

+ Chia sẻ, lan tỏa các thông tin tích cực; cảnh báo và phản ánh, tố giác các hành vi vi phạm pháp luật.

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

- Tham gia xây dựng 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.

- Kiểm tra, đánh giá các doanh nghiệp trên địa bàn cung cấp dịch vụ xuyên biên giới đối với việc tuân thủ quy định của pháp luật về lưu trữ, xử lý dữ liệu của tổ chức, cá nhân.

- Bảo đảm an ninh mạng, an toàn thông tin mạng theo cấp độ cho các cơ sở dữ liệu cấp tỉnh và cơ sở dữ liệu quan trọng của các sở, ngành, lĩnh vực liên quan.

- Căn cứ các quy định, hướng dẫn của các Bộ, Ngành: Đánh giá rủi ro bảo mật dữ liệu tập trung, hiệu quả và có thẩm quyền; báo cáo, chia sẻ thông tin, giám sát và cảnh báo sớm; thu thập, phân tích, nghiên cứu, phán đoán và cảnh báo sớm về thông tin rủi ro 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[3]

- 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.

---

[3] Theo Điều 3, 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 quy định: "Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin. Đối với cơ quan, tổ chức nhà nước, chủ quản hệ thống thông tin là các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương hoặc là cấp có thẩm quyền quyết định đầu tư dự án xây dựng, thiết lập, nâng cấp, mở rộng hệ thống thông tin đó".

- 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 1 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 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.

b) Công an tỉnh

- Căn cứ các quy định của Chính phủ, Bộ Công an: Xây dựng quy trình 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.

- Tham gia xây dựng cơ chế 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 sở, ban, ngành trên địa bàn khi có đề nghị của chủ quản hệ thống thông tin. Căn cứ các quy định của Nhà nước, tổ chức đánh giá, xếp hạng mức độ an ninh mạng đối với hệ thống thông tin của sở, ban, ngành trên địa bàn.

- Tổ chức diễn tập thực chiến về an ninh mạng cấp tỉnh, có sự tham gia của các chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, sở, ban, ngành, tổ chức, doanh nghiệp bảo đảm an ninh mạng.

- Xây dựng, hình thành mạng lưới ứng phó, khắc phục sự cố an ninh mạng cấp tỉnh, 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 trên địa bàn.

- Chủ trì, phối hợp với Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông, các sở, ngành có liên quan xây dựng cơ chế phối hợp, chia sẻ thông tin giám sát an toàn, an ninh mạng hệ thống thông tin của các sở, ban, ngành, địa phương, tổ chức, doanh nghiệp trọng yếu trên địa bàn.

- 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, hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quân sự theo chức năng, nhiệm vụ được giao.

- Tham mưu, 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

- Căn cứ các hướng dẫn của Chính phủ, Bộ Thông tin và Truyền thông: Triển khai Nền tảng điện toán đám mây riêng của Chính phủ đáp ứng yêu cầu bảo đảm an toàn thông tin mạng, tạo cơ sở hạ tầng an toàn cho các ứng dụng Chính phủ điện tử dùng chung.

- Tổ chức đánh giá, xếp hạng mức độ an toàn thông tin của các cơ quan, tổ chức, doanh nghiệp nhà nước và các tổ chức, doanh nghiệp trên địa bàn hoạt động trong các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng.

- Triển khai các biện pháp kỹ thuật phục vụ bảo đảm an toàn thông tin cho quá trình chuyển đổi số quốc gia, phát triển kinh tế số, xã hội số trên địa bàn.

đ) Phòng Cơ yếu - CNTT trực thuộc Văn phòng Tỉnh ủy

- Triển khai giải pháp dùng mật mã để bảo vệ thông tin trong hệ thống thông tin quan trọng quốc gia của các cơ quan Đảng, Nhà nước theo hướng dẫn của Ban Cơ yếu Chính phủ.

- Cung cấp dịch vụ và quản lý hệ thống chứng thực chữ ký số chuyên dùng phục vụ các cơ quan thuộc hệ thống chính trị, triển khai bảo mật ứng dụng công nghệ thông tin trong hoạt động của các cơ quan Đảng, Nhà nước trên địa bàn, đáp ứng yêu cầu bảo mật và an toàn thông tin cho Chính phủ điện tử.

- Phối hợp với các cơ quan liên quan triển khai giám sát an toàn thông tin trên hệ thống thông tin quan trọng quốc gia của các cơ quan Đảng, Nhà nước trên địa bàn.

e) Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Sở Thông tin và Truyền thông thực hiện giám sát, cảnh báo sớm để bảo vệ hệ thống thông tin của các cơ quan Đảng, Nhà nước theo chức năng, nhiệm vụ được giao.

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.

- Tối thiểu 1 năm/1 lần tổ chức diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn thông tin cho các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin và hệ thống thông tin quan trọng quốc gia.

- Phát triển các Đội ứng cứu sự cố khẩn cấp thuộc lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (CERT lĩnh vực) theo sự điều phối của Sở Thông tin và Truyền thông, tham gia vào Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia.

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

c) Công an tỉnh hướng dẫn, đôn đốc, 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 sự tỉnh hướng dẫn, đôn đốc, 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, đôn đốc, kiểm tra công tác bảo đảm an toàn thông tin mạng và ứng cứu sự cố đối với các hệ thống thông tin thuộc các lĩnh vực 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

- Căn cứ hướng dẫn của Bộ Công an, triển khai 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 quần 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 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 trên địa bàn.

- Xây dựng cơ chế phối hợp liên ngành với các sở, ngành, Ủy ban nhân dân các huyện, thị xã, thành phố, giữa lực lượng chuyên trách bảo vệ an ninh mạng với các tổ chức, doanh nghiệp trên địa bàn 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.

- 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.

- Phối hợp với các sở, ngành liên quan, tham gia xây dựng hệ thống cảnh báo sớm cấp tỉnh để kịp thời phát hiện, điều phối, ứng cứu cố sự an ninh mạng; thu thập, chia sẻ thông tin về an ninh mạng giữa Nhà nước và doanh nghiệp, trong nước và thế giới; xây dựng, hình thành nền tảng điều hành, giám sát an ninh mạng thống nhất.

b) Sở Thông tin và Truyền thông

- Thúc đẩy phát triển ứng dụng (app) Internet an toàn nhằm bảo vệ người dân 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 trên địa bàn 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. 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 cẩm nang hướng dẫn các tổ chức, doanh nghiệp trên địa bàn triển khai giải pháp bảo đảm an toàn thông tin mạng.

- Thực hiện 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 theo hướng dẫn của Bộ Thông tin và Truyền thông.

c) Bộ Chỉ huy Quân sự tỉnh

- Tham gia 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.

- 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, Ủy ban nhân dân các huyện, thị xã, thành phố 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, ngành, Ủy ban nhân dân các huyện, thị xã, thành phố

- 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

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 theo hướng dẫn của Bộ thông tin và Truyền thông.

- Nghiên cứu phát triển đội ngũ chuyên gia về an toàn thông tin, an ninh mạng để giải quyết các bài toán khó xảy ra trên địa bàn.

- 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.

- 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 quốc gia trên địa bàn.

b) Công an tỉnh

- Triển khai thực hiện cơ chế, chính sách, pháp luật về đào tạo nguồn nhân lực về bảo đảm an ninh mạng theo hướng dẫn của Bộ Công an.

- Chủ động phát hiện, đào tạo tài năng trẻ về an ninh mạng. Phối hợp các đơn vị nghiệp vụ trực thuộc Bộ Công an có chính sách ưu tiên đào tạo các tài năng trẻ, tạo điều kiện để du học nước ngoài, tài trợ nghiên cứu ở nước ngoài để về nước phát triển nền an ninh mạng quốc gia. Tăng cường tổ chức các hội nghị, hội thảo về an ninh mạng quốc tế trên địa bàn tỉnh nhằm phát huy vai trò của các nhà khoa học về an ninh mạng đồng thời tạo môi trường phát triển cho các tài năng trẻ.

- Tạo môi trường phát triển cạnh tranh, bình đẳng giữa doanh nghiệp an ninh mạng trong nước và nước ngoài.

- Triển khai Đề án "Đào tạo nguồn nhân lực an ninh mạng đến năm 2025, tầm nhìn đến năm 2030" theo hướng dẫn của Bộ Công an.

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

c) Bộ Chỉ huy Quân sự tỉnh

- Chủ trì, phối hợp với các sở, ngành 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 theo hướng dẫn của Bộ Quốc phòng.

- Triển khai thực hiện các Đề án của Bộ Quốc phòng về 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 không gian mạng; tham gia 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.

9. 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" theo hướng dẫn của Bộ Thông tin và Truyền thông.

- 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.

- Tham gia xây dựng, hoàn thiện các cơ chế, chính sách và thiết lập các

kênh liên hệ, trao đổi để người sử dụng có thể thuận lợi phản ánh, chia sẻ và chung tay bảo đảm an toàn thông tin mạng quốc gia.

- 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

- Xây dựng và triển khai Đề án "Tuyên truyền, nâng cao nhận thức và phổ biến kiến thức về an ninh mạng" theo hướng dẫn của Bộ Công an.

- Tổ chức tuyên truyền, nâng cao nhận thức, kiến thức về bảo đảm an ninh mạng hàng năm, có quy mô lớn, trên địa bàn tỉnh, với sự tham gia của các phương tiện truyền thông, báo chí, cơ quan, tổ chức, doanh nghiệp từ cấp tỉnh tới cấp huyện, thị xã, thành phố.

- 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.

- Tham gia xây dựng, ban hành Bộ kỹ năng bảo đảm an ninh mạng khi tham gia không gian mạng.

c) Cơ quan, tổ chức, doanh nghiệp

- 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.

- Các cơ sở giáo dục, đào tạo xây dựng chương trình, kế hoạch học tập, rèn luyện kỹ năng tư duy phản biện 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 trong và ngoài nước 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, 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.

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

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.

b) 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.

c) Xây dựng 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.

d) Ưu tiên bố trí nguồn lực để triển khai các Đề án và xây dựng các hệ thống kỹ thuật bảo đảm an toàn, an ninh mạng quy mô quốc gia.

đ) 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.

e) Phân bổ ngân sách bảo đảm kinh phí thực hiện các nhiệm vụ theo nội dung Kế hoạch do các sở, ngành liên quan thực hiện.

g) Ưu tiên nguồn vốn khoa học và công nghệ, nguồn vốn từ các chương trình quốc gia để phát triển công nghệ cao, chương trình phát triển sản phẩm quốc gia để phát triển sản phẩm, dịch vụ, giải pháp nội địa và các nhiệm vụ nghiên cứu, phát triển, chuyển giao công nghệ theo Kế hoạch đề ra.

III. TỔ CHỨC THỰC HIỆN

1. Tiểu ban An toàn, An ninh mạng tỉnh

a) Giúp Chủ tịch Ủy ban nhân dân tỉnh, Trưởng Tiểu ban An toàn, An ninh mạng tỉnh chỉ đạo sơ kết, tổng kết việc thực hiện Kế hoạch triển khai thực hiện Quyết định số 964/QĐ-TTg trên địa bàn tỉnh.

b) Đề xuất với Chủ tịch Ủy ban nhân dân 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 trong nội dung của Kế hoạch, cần sự phối hợp giữa các sở, ngành, cơ quan chức năng trên địa bàn tỉnh.

2. Công an tỉnh

a) Chủ trì, phối hợp hướng dẫn, đôn đốc, kiểm tra các cơ quan, tổ chức, doanh nghiệp trên địa bàn triển khai thực hiện các nội dung về an ninh mạng tại Kế hoạch; tổ chức sơ kết, tổng kết, tổng hợp, báo cáo Chủ tịch Ủy ban nhân dân tỉnh tình hình thực hiện và đề xuất, kiến nghị nhiệm vụ mới cho phù hợp với tình hình thực tiễn tại địa phương đối với các nội dung về an ninh mạng thuộc Kế hoạch.

b) Chủ trì, phối hợp với các sở, ngành, tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ đã giao Công an tỉnh tại phần II; thực hiện nhiệm vụ tại Mục 1, điểm d Mục 2, Mục 3, các điểm a và điểm d Mục 4, điểm e Mục 5, điểm b Mục 6 phần II theo chức năng, nhiệm vụ được giao.

c) Xây dựng phương án bảo đảm an ninh chính trị nội bộ, an ninh kinh tế tại các cơ quan, đơn vị 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.

3. Sở Thông tin và Truyền thông

a) Chủ trì, phối hợp, hướng dẫn, đôn đốc, kiểm tra các cơ quan, tổ chức, doanh nghiệp tổ chức triển khai thực hiện các nội dung về an toàn thông tin mạng tại Kế hoạch này; tổ chức sơ kết, tổng kết, tổng hợp, báo cáo Thủ tướng Chính phủ 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 toàn thông tin mạng thuộc Kế hoạch.

b) Chủ trì, phối hợp với các sở, ngành, địa phương và tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ đã giao Sở Thông tin và Truyền thông tại phần II; thực hiện nhiệm vụ tại Mục 1, điểm d Mục 2, Mục 3, các điểm a và điểm d Mục 4, điểm e Mục 5, điểm b Mục 6 phần II theo chức năng, nhiệm vụ được giao.

4. Bộ Chỉ huy Quân sự tỉnh

a) Thực hiện phòng ngừa, ứng phó, xử lý các nguy cơ, thách thức từ không gian mạng theo chức năng, nhiệm vụ được giao.

b) Chủ trì, phối hợp với các sở, ngành, địa phương và tổ chức, doanh nghiệp liên quan thực hiện các nhiệm vụ đã giao Bộ Chỉ huy Quân sự tỉnh tại phần II; thực hiện nhiệm vụ tại Mục 1, điểm d Mục 2, Mục 3, các điểm a và điểm d Mục 4, điểm e Mục 5, điểm b Mục 6 phần II theo chức năng, nhiệm vụ được giao.

5. 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 tham gia nghiên cứu, thực hiện chuyển giao công nghệ và xây dựng, ban hành các tiêu chuẩn kỹ thuật về an toàn, an ninh mạng theo hướng dẫn của Bộ Khoa học và Công nghệ.

6. Sở Nội vụ

Chủ trì, phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông, Bộ Tài chính áp dụng 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 Bộ Nội vụ.

7. Sở Kế hoạch và Đầu tư, Sở Tài chính ưu tiên bố trí kinh phí từ ngân sách của tỉnh để triển khai các nhiệm vụ của Kế hoạch theo quy định của pháp luật về đầu tư công, pháp luật về ngân sách nhà nước.

8. Các sở, ban, ngành, Ủy ban nhân dân các huyện, thị xã, thành phố

a) Phối hợp Công an tỉnh, Sở Thông tin và Truyền thông tổ chức thực hiện các nhiệm vụ được giao tại Kế hoạch.

b) 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 của Công an tỉnh, Sở Thông tin và Truyền thông và quy định của pháp luật; ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an toàn thông tin mạng "Make in Viet Nam", an ninh mạng tự chủ. 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.

c) 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. Tăng cường hoạt động thanh tra, kiểm tra, công bố và xử lý nghiêm các hành vi vi phạm.

d) Chỉ đạo các công ty, doanh nghiệp, đơn vị 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 điều khiển công nghiệp và các hệ thống thông tin quan trọng khác do doanh nghiệp quản lý, vận hành, khai thác.

đ) 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, tổ chức và lĩnh vực quản lý.

e) Kiểm tra, đánh giá và báo cáo hàng năm ***(trước ngày 10/10)*** hoặc đột xuất theo hướng dẫn của Công an tỉnh, Sở Thông tin và Truyền thông về tình hình, kết quả triển khai thực hiện Kế hoạch để tổng hợp, báo cáo Chủ tịch Ủy ban nhân dân tỉnh theo quy định về chế độ báo cáo.

9. Phòng Cơ yếu - CNTT trực thuộc Văn phòng Tỉnh ủy

a) Triển khai hạ tầng mật mã quốc gia để bảo vệ thông tin phục vụ lãnh đạo, chỉ đạo, chỉ huy của Đảng, Nhà nước được truyền, lưu giữ trên không gian mạng theo hướng dẫn của Ban Cơ yếu Chính phủ.

b) Chủ trì, phối hợp với Sở Thông tin và Truyền thông, các cơ quan liên quan trên địa bàn tỉnh bảo đảm bảo mật, an toàn thông tin cho các hệ thống thông tin của các cơ quan Đảng, Nhà nước theo quy định của pháp luật về cơ yếu.

10. Các tập đoàn, công ty, doanh nghiệp nhà nước trên địa bàn

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, Sở Thông tin và Truyền thông.

11. Các doanh nghiệp viễn thông, Internet, doanh nghiệp chủ quản nền tảng số

a) Chủ động, tích cực phối hợp triển khai công tác bảo đảm an toàn, an ninh mạng trong hoạt động của doanh nghiệp; phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông trong triển khai thực các nhiệm vụ tại Kế hoạch.

b) 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.

c) Vận động các hội viên tích cực nghiên cứu, phát triển các sản phẩm, dịch vụ, giải pháp an toàn, an ninh mạng hiệu quả, chất lượng; ưu tiên sử dụng sản phẩm, dịch vụ, giải pháp an toàn thông tin mạng "Make in Viet Nam".

d) Định kỳ hàng năm ***(trước ngày 10/10)*** 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./.

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Công an; (để báo cáo)
- TT Tỉnh ủy, HĐND tỉnh;
- Ban Tuyên giáo Tỉnh ủy (để phối hợp thực hiện);
- CT, PCT UBND tỉnh (đ/c Võ Văn Cảnh);
- Phòng Cơ yếu - CNTT thuộc VPTU;
- Các sở, ban, ngành của tỉnh;
- UBND các huyện, thị xã, thành phố; (để thực hiện)
- Các doanh nghiệp viễn thông, internet;
- Phó CVP UBND tỉnh (đ/c Nguyễn Tiến Dũng);
- Tiểu ban AT, ANM (TGV-PA05);
- Các Phòng: TH, HCTC QC45d;
- Trung tâm CN&CTTĐT tỉnh;
- Lưu: VT, NC (w.20b).

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Võ Văn Cảnh