UBND TỈNH BẮC GIANG
SỞ KHOA HỌC VÀ CÔNG NGHỆ

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 139/KH-KHCN

Bắc Giang, ngày 14 *tháng 11 năm 2022*

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

Thực hiện Kế hoạch số 5603/KH-UBND ngày 08/11/2022 của Chủ tịch UBND tỉnh về việc triển khai thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứngphó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030, Sở Khoa học và Công nghệ xây dựng Kế hoạch cụ thể như sau:

I. MỤC TIÊU, YÊU CẦU

1. Mục tiêu

a) Mục tiêu tổng quát

Xây dựng, phát triển 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 thông tin mạng và an ninh mạng (gọi tắt là an toàn, an ninh mạng) được nâng cao, chủ động, sẵn sàng ứng phó với các nguy cơ, thách thức từ không gianmạng 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, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

b) Mục tiêu cụ thể đến năm 2025

- Xây dựng Thế trận An ninh nhân dân trên không gian mạng có khả năng chỉ huy, kết nối, chia sẻ thông tin, tiếp nhận và xử lý sớm các thông tin gây hại tới không gian mạng quốc gia từ các bộ, ngành, địa phương, các doanh nghiệp viễn thông, Internet, dịch vụ nội dung số.

- Hình thành lực lượng bảo đảm an toàn, an ninh mạng của sở, đảm nhận nhiệm vụ làm đầu mối, chịu trách nhiệm về công tác bảo đảm an toàn, an ninh mạng.

- Bảo vệ cơ sở hạ tầng không gian mạng, trọng tâm là hệ thống thông tin quan trọng về an ninh quốc gia theo quy định của pháp luật về an ninh mạng. Bảovệ hệ thống thông tin của 11 lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng (theo Quyết định số 632/QĐ-TTg của Thủ tướng Chính phủ).

- Phấn đấu 100% công chức, viên chức, người lao động sử dụng Internet có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

- Áp dụng chính sách phù hợp cho thúc đẩy khởi nghiệp về an toàn, an ninh mạng góp phần xây dựng nền móng hình thành nền công nghiệp an ninh mạng và công nghiệp an toàn thông tin mạng.

- Kinh phí bảo đảm 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.

c) Mục tiêu cụ thể đến năm 2030

- Góp phần duy trì, nâng cao năng lực, thứ hạng về an toàn, an ninh mạngcủa Việt Nam trên bảng xếp hạng toàn cầu.

- Xây dựng được Thế trận An ninh nhân dân trên không gian mạng với sự tham gia đông đảo, tích cực của công chức, viên chức, người lao động.

- Củng cố, tăng cường lực lượng bảo đảm an toàn, an ninh mạng.

- Phấn đấu 90% công chức, viên chức, người lao động sử dụng Internet có cơ hội tiếp cận hoạt động nângcao nhận thức, kỹ năng và công cụ bảo đảm an toàn, an ninh mạng.

2. Yêu cầu

a) Bảo đảm an toàn, an ninh mạng trở thành công tác trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số; là nhiệm vụ trọng yếu, thường xuyên, lâu dài nhằm khởi tạo và duy trì môi trường mạng an toàn, lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và mỗi người dân.

b) Kịp thời nắm bắt, tận dụng hiệu quả các cơ hội do không gian mạng mang lại để phát triển kinh tế, xã hội, đồng thời 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 tính bền vững của quá trình phát triển đất nước trong thời đại Cách mạng công nghiệp lần thứ tư.

c) Phát huy sức mạnh của cả hệ thống chính trị và toàn xã hội, chủ động ứng phó từ sớm, từ xa với các nguy cơ, thách thức, hoạt động gây tổn hại tới chủquyền, lợi ích, an ninh quốc gia trên không gian mạng và an toàn thông tin mạngquốc gia, trong đó cơ quan quản lý nhà nước giữ vai trò điều phối, gắn kết, chia sẻ thông tin. 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. Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông 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 khônggian mạng.

d) 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.

đ) Thúc đẩy nghiên cứu, phát triển về công nghệ, sản phẩm, dịch vụ an toàn,an ninh mạng là giải pháp căn cơ bảo đảm an toàn, an ninh mạng quốc gia; phát triển thị trường, doanh nghiệp, năng lực cạnh tranh về an toàn, an ninh mạng, gópphần đưa

nước ta trở thành quốc gia tự chủ, có năng lực cao về bảo đảm an toàn,an ninh mạng; đầu tư cho an toàn, an ninh mạng là đầu tư cho phát triển bền vững và tạo ra giá trị. Chủ động làm bạn, đối tác tin cậy, có trách nhiệm với các doanhnghiệp, tổ chức nước ngoài trong lĩnh vực an toàn, an ninh mạng.

e) Bảo đảm sự lãnh đạo toàn diện của các cấp ủy Đảng, chính quyền trong công tác bảo đảm an toàn, an ninh mạng, chủ động ứng phó với các thách thức từkhông gian mạng. Xây dựng lực lượng bảo đảm an toàn, an ninh mạng hiện đại, chuyên nghiệp, có đủ nguồn nhân lực chất lượng cao đáp ứng yêu cầu thực tiễn.

II. NỘI DUNG THỰC HIỆN

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

- Thường xuyên phổ biến, quán triệt chủ trương, đường lối 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, công chức, viên chức, người lao động, người dân, doanh nghiệp trong công tác bảo đảm an toàn, an ninh mạng. Lãnh đạo Sở, Trưởng các phòng, đơn vị thuộc Sở 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.

- Xây dựng Thế trận An ninh nhân dân trên không gian mạng kết hợp chặtchẽ với Thế trận Quốc phòng toàn dân trên không gian mạng.

- Phát huy sự tham gia có hiệu quả của công chức, viên chức, người lao động 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.

2. Hoàn thiện văn bản về an toàn, an ninh mạng

Phối hợp với Công an tỉnh, Sở Thông tin và Truyền thông rà soát, sửa đổi, bổ sung văn bản về bảo đảm an toàn, anninh mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, bảo vệ thông tin cá nhân trên mạng bảo đảm phù hợp với các văn bản quy phạm pháp luật hiện hành về an toàn, an ninh mạng.

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

a) Bảo vệ cơ sở hạ tầng số

- Đẩy mạnh hoạt động bảo đảm an toàn, an ninh mạng trong quá trình vận hành, khai thác cơ sở hạ tầng số; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an, Sở Thông tin và Truyền thông và quy định của pháp luật về an toàn, an ninh mạng; gắn kết công tác bảo đảm an toàn, an ninh mạng với công tác triển khai chuyển đổi số, ứng dụng côngnghệ thông tin, phát triển chính quyền điện tử hướng tới chính quyền số, phát triển đô thị thông minh, kinh tế số và xã hội số.

- Bảo đảm an toàn, an ninh mạng cho quá trình triển khai Chính quyền điệntử, chuyển đổi số.

b) Bảo vệ nền tảng số

- Chủ động giám sát, phát hiện và công bố hành vi vi phạm quy định pháp luật của Việt Nam thuộc phạm vi quản lý trên các nền tảng số.

- Phối hợp với các cơ quan chức năng có thẩm quyền rà soát, phát hiện và xử lý thông tin, tổ chức, cá nhân vi phạm pháp luật trên môi trường mạng thuộc lĩnh vực an toàn, an ninh mạng; tăng cường hoạt động thanh tra, kiểm tra, công bố và xử lý nghiêm các hành vi vi phạm.

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

- Cập nhật, tiếp nhận, xử lý các cảnh báo về thông tin rủi ro bảo mật dữ liệu.

- Rà soát theo cấp độ cho các cơ sở dữ liệu quan trọng theo quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ.

4. Hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh; nhất là bảo vệ hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin

- Nâng cao trách nhiệm tự bảo vệ hệ thống thông tin thuộc phạm vi quản lý.

- Xây dựng, cập nhật, vận hành hệ thống thông tin theo tiêu chuẩn, quychuẩn kỹ thuật về an toàn, an ninh mạng.

- Phối hợp 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 04 lớp trước khi đưa vào sử dụng.

- Chủ động thường xuyên 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 công chức, viên chức và người lao động.

- Tham gia diễn tập, ứng phó và ứng cứu sự cố an toàn, an ninh mạng; nhất là 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.

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

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 ninhnhân dân trên không gian mạng. 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 phápluật trong phạm vi quản lý.

- Yêu cầu công chức, viên chức, người lao động đăng tải các nội dung trên

mạng xã hội chính xác và tích cực; phản bác hiệu quả các thông tin tiêu cực về đất nước, con người Việt Nam.

6. Kinh phí

- Bố trí đủ nhân lực chuyên trách, chịu trách nhiệm về an toàn, an ninh mạng; 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 Sở.

- Bố trí kinh phí chi cho an toàn, an ninh mạng đạt tối thiểu 10% kinh phí chi cho chuyển đổi số, ứng dụng công nghệ thông tin.

III. TỔ CHỨC THỰC HIỆN

1. Các phòng, đơn vị căn cứ Kế hoạch để tổ chức triển khai, thực hiện công việc đảm bảo an toàn, an ninh thông tin; chủ động phối hợp cung cấp thông tin khi có yêu cầu.

2. Văn phòng Sở chủ trì theo dõi, đôn đốc các phòng, đơn vị triển khai thực hiện các nhiệm vụ về an toàn thông tin mạng tại Kế hoạch này.

- Căn cứ khả năng cân đối ngân sách ưu tiên bố trí kinh phí từ NSNN để triển khai các nhiệm vụ của Kế hoạch theo quy định của pháp luật về NSNN và đầu tư công.

- Theo dõi, kiểm tra, đánh giá, đôn đốc các phòng, đơn vị triển khai thực hiện có hiệu quả công tác bảo đảman ninh mạng. Định kỳ, đột xuất tổng hợp tình hình, kết quả báo cáo Giám đốc Sở theo quy định.

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 của Sở Khoa học và Công nghệ./.

Nơi nhận:
- Công an tỉnh (Báo cáo);
- Sở TT&TT;
- Lãnh đạo Sở;
- Các phòng, đơn vị thuộc Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ KHOA HỌC VÀ CÔNG NGHỆ
TỈNH BẮC GIANG

Nguyễn Thanh Bình