

Số: 775 /KH-UBND

Nghệ An, ngày 49 tháng 9 năm 2025

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng
trên địa bàn tỉnh Nghệ An

Thực hiện Nghị quyết số 71/NQ-CP ngày 01/4/2025 của Chính phủ sửa đổi, bổ sung cập nhật chương trình hành động của Chính phủ thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia; Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; UBND tỉnh ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Nghệ An như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin (viết tắt là ATTT) cho các hệ thống thông tin (viết tắt là HTTT) quan trọng trên địa bàn tỉnh; bảo đảm khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ đe dọa mất ATTT trên mạng; đề ra các giải pháp ứng phó khi gặp sự cố mất ATTT mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về ATTT đối với lực lượng cán bộ, công chức, viên chức trong các cơ quan nhà nước tỉnh.

- Xây dựng đội ứng cứu sự cố có đủ kiến thức, kỹ năng xử lý sự cố ATTT mạng đảm bảo linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- Bảo đảm các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố ATTT mạng.

2. Yêu cầu

- Các HTTT của các cơ quan, đơn vị, địa phương phải được đánh giá hiện trạng và khả năng bảo đảm ATTT mạng, dự báo các nguy cơ, sự cố mất ATTT mạng của HTTT của các cơ quan nhà nước trên địa bàn tỉnh để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

- Hoạt động ứng cứu sự cố ATTT mạng phải chuyển từ bị động sang chủ động, bao gồm: chủ động thực hiện sẵn lòng mỗi nguy hại và rà quét lỗ hổng trên các HTTT trong phạm vi quản lý.

- Xác định cụ thể các nguồn lực đảm bảo, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, đảm bảo khả thi, hiệu quả.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm ATTT giữa các cơ quan nhà nước trên địa bàn tỉnh; tận dụng sự phối hợp, hỗ trợ của Cơ quan điều phối quốc gia về ứng cứu sự cố (*Trung tâm An ninh mạng quốc gia - Bộ Công an*).

II. CÁC QUY ĐỊNH CHUNG

1. Phạm vi và đối tượng

Kế hoạch này để ứng phó sự cố, bảo đảm ATTT mạng đối với các HTTT của tỉnh, áp dụng cho các sở, ban, ngành cấp tỉnh; UBND các xã, phường; các cơ quan, đơn vị, doanh nghiệp có liên quan (*gọi tắt là cơ quan, đơn vị, địa phương*).

2. Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố ATTT mạng.
- Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả; phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan, đơn vị.
- Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản HTTT.
- Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của HTTT đã được cấp thẩm quyền phê duyệt trong Kế hoạch ứng phó sự cố.
- Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.
- Bảo đảm bí mật thông tin biết được khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của Cơ quan điều phối quốc gia hoặc cơ quan, tổ chức, cá nhân gặp sự cố.
- Công tác ứng phó sự cố ATTT mạng phải tuân thủ theo Quy trình ứng cứu sự cố thông thường quy định tại Phụ lục II kèm theo Thông tư số 20/2017/TT-BTTTT, Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và các văn bản quy định khác có liên quan.

3. Các lực lượng tham gia ứng phó sự cố

- Các sở, ban, ngành của tỉnh, UBND các xã, phường và các cơ quan, đơn vị, doanh nghiệp có liên quan.
- Đội ứng cứu sự cố An ninh mạng tỉnh (*lực lượng chính thực hiện công tác ứng phó sự cố, trong đó Công an tỉnh là cơ quan thường trực*).
- Chủ quản HTTT; đơn vị quản lý, vận hành HTTT.
- Trung tâm Khoa học công nghệ và Truyền thông thuộc Sở Khoa học và Công nghệ.
- Doanh nghiệp cung cấp dịch vụ viễn thông internet (*VNPT, Viettel, FPT, Mobifone...*).
- Doanh nghiệp cung cấp dịch vụ ATTT mạng (*trường hợp thuê dịch vụ*).
- Trong trường hợp cần thiết, mời các cơ quan Trung ương có chức năng cùng tham gia.

4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các cơ quan, đơn vị

- Công an tỉnh: Đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh; thực hiện chỉ đạo, tổ chức triển khai hoạt động ứng phó sự cố ATTT mạng và các nhiệm vụ khác khi xảy ra sự cố.

- Đội ứng cứu sự cố an ninh mạng của tỉnh: Lực lượng chính tham gia hoạt động ứng cứu sự cố ATTT mạng, thực hiện nhiệm vụ theo Quy chế hoạt động của Đội, tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia khi có yêu cầu từ Bộ Công an hoặc các bộ, ngành có liên quan.

- Trung tâm Khoa học công nghệ và Truyền thông - Sở Khoa học và Công nghệ: Nghiên cứu, cập nhật các giải pháp quản lý, vận hành hạ tầng mạng truyền số liệu dùng chung, kho dữ liệu tỉnh; tham gia Đội ứng cứu sự cố an ninh mạng của tỉnh, xử lý, ứng cứu các sự cố về an ninh mạng, ATTT xảy ra trên địa bàn tỉnh khi có yêu cầu của đơn vị điều phối.

- Các cơ quan, đơn vị: Có trách nhiệm cử cán bộ, công chức, viên chức phụ trách ATTT tham gia Đội ứng cứu sự cố an ninh mạng của tỉnh khi xử lý sự cố. Phối hợp với các đơn vị chuyên trách ứng cứu sự cố ATTT mạng của tỉnh trong công tác ứng phó, xử lý các sự cố.

- Doanh nghiệp cung cấp, xây dựng các HTTT: Phối hợp với Công an tỉnh, chủ quản HTTT, đơn vị vận hành HTTT trong công tác ứng phó, xử lý các sự cố ATTT liên quan HTTT do mình xây dựng hoặc cung cấp.

- Doanh nghiệp cung cấp dịch vụ viễn thông internet: Phối hợp với Công an tỉnh, chủ quản HTTT, đơn vị quản lý, vận hành HTTT trong công tác ứng phó, xử lý các sự cố ATTT liên quan đến hạ tầng viễn thông, dịch vụ internet do mình cung cấp hoặc quản lý.

III. NỘI DUNG THỰC HIỆN

1. Đánh giá các nguy cơ, sự cố ATTT mạng

1.1. Nội dung thực hiện: Đánh giá hiện trạng và khả năng bảo đảm ATTT mạng của các HTTT và các đối tượng cần bảo vệ thuộc phạm vi của Kế hoạch; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các HTTT và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

- Đơn vị chủ trì: Đơn vị quản lý, vận hành HTTT.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố an ninh mạng của tỉnh; Trung tâm Khoa học công nghệ và Truyền thông - Sở Khoa học và Công nghệ; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (*trường hợp thuê dịch vụ*) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

1.2. Nội dung thực hiện: Chủ động thực hiện sẵn lòng mỗi nguy hại và rà

quét lỗ hổng trên các HTTT trong phạm vi quản lý; khắc phục các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng (*thực hiện theo quy định tại Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ*).

- Đơn vị chủ trì: Đơn vị quản lý, vận hành HTTT.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố An ninh mạng của tỉnh; Trung tâm Khoa học công nghệ và Truyền thông (Sở Khoa học và Công nghệ); các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (*trường hợp thuê dịch vụ*) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: hàng năm (*tối thiểu 01 lần/06 tháng*).

2. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi HTTT, chương trình ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

2.1. Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu khi HTTT gặp sự cố, có phân theo các loại sự cố thực hiện theo mục 3, Phần III. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố của Kế hoạch này.

2.2. Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp. Các sự cố thường gặp:

- Sự cố do bị tấn công mạng;
- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...;
- Sự cố do lỗi của người quản trị, vận hành hệ thống;
- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

2.3. Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống sau:

- Tình huống sự cố do bị tấn công mạng:
 - + Tấn công từ chối dịch vụ;
 - + Tấn công giả mạo;
 - + Tấn công sử dụng mã độc;
 - + Tấn công truy cập trái phép, chiếm quyền điều khiển;
 - + Tấn công thay đổi giao diện;
 - + Tấn công mã hóa phần mềm, dữ liệu, thiết bị;
 - + Tấn công phá hoại thông tin, dữ liệu, phần mềm;
 - + Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;
 - + Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

ng

- + Các hình thức tấn công mạng khác.
- Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:
- + Sự cố nguồn điện;
- + Sự cố đường kết nối Internet;
- + Sự cố do lỗi phần mềm, phần cứng, ứng dụng của HTTT;
- + Sự cố liên quan đến quá tải hệ thống;
- + Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.
- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống:
- + Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;
- + Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;
- + Lỗi liên quan đến chính sách và thủ tục ATTT;
- + Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;
- + Lỗi khác liên quan đến người quản trị, vận hành hệ thống.
- Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

2.4. Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, giữa các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

- Đơn vị chủ trì: Công an tỉnh.
- Đơn vị phối hợp: Cơ quan điều phối quốc gia Trung tâm An ninh mạng quốc gia; các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; Đội ứng cứu sự cố An ninh mạng của tỉnh; Trung tâm Khoa học công nghệ và Truyền thông (*Sở Khoa học và Công nghệ*); các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (*trường hợp thuê dịch vụ*) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hằng năm.

2.5. Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ, và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

- Đơn vị chủ trì: Các sở, ban, ngành của tỉnh, UBND các xã, phường.
- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố An ninh mạng của tỉnh; Trung tâm Khoa học công nghệ và Truyền thông (*Sở Khoa học và Công nghệ*); các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (*trường hợp thuê dịch vụ*) và các cơ quan, đơn vị khác có liên quan.
- Thời gian thực hiện: Thường xuyên hằng năm.

3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

3.1. Thông báo, báo cáo sự cố ATTT mạng

- Đơn vị thực hiện: Đơn vị quản lý, vận hành HTTT báo cáo Cơ quan chủ quản HTTT; Công an tỉnh; Đội ứng cứu sự cố An ninh mạng của tỉnh; đồng gửi Cơ quan điều phối quốc gia (*Trung tâm An ninh mạng quốc gia*).

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

3.2. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng

- Đơn vị thực hiện: Công an tỉnh; Đơn vị quản lý, vận hành HTTT (các cơ quan, đơn vị); Đội ứng cứu sự cố an ninh mạng của tỉnh; Trung tâm Khoa học công nghệ và Truyền thông - Sở Khoa học và Công nghệ.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (*Trung tâm An ninh mạng quốc gia*); tổ chức, cá nhân gửi thông báo, báo cáo sự cố; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (*trường hợp thuê dịch vụ*) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

3.3. Quy trình ứng cứu sự cố ATTT mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 11 Thông tư số 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (*Sơ đồ, biểu mẫu tại phụ lục kèm theo Kế hoạch*).

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; Đơn vị quản lý, vận hành HTTT; Đội ứng cứu sự cố An ninh mạng của tỉnh; Trung tâm Khoa học công nghệ và Truyền thông - Sở Khoa học và Công nghệ.

- Thời gian thực hiện: Hằng năm.

4. Triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố. Đồng thời cần đáp ứng đúng theo quy định tại Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm ATTT mạng, cụ thể bao gồm:

4.1. Triển khai các chương trình huấn luyện, diễn tập:

- Nội dung thực hiện: Tổ chức diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Công an tỉnh; Đội ứng cứu sự cố an ninh mạng của tỉnh.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành HTTT; Cơ quan điều phối quốc gia (*Trung tâm An ninh mạng quốc gia*); các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (*trường hợp thuê dịch vụ*) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Hằng năm.

4.2. Triển khai nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố.

- Nội dung thực hiện: Thực hiện nghiêm túc công tác giám sát, phát hiện

sớm nguy cơ, sự cố; kiểm tra, đánh giá ATTT mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro ATTT mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn ATTT; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Đơn vị chủ trì: Công an tỉnh; Đơn vị quản lý, vận hành HTTT; Đội ứng cứu sự cố an ninh mạng của tỉnh; Trung tâm Khoa học công nghệ và Truyền thông - Sở Khoa học và Công nghệ.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Thường xuyên, hằng năm.

4.3. Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố:

- Nội dung thực hiện: Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của đội ứng cứu sự cố, bộ phận ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Đơn vị chủ trì: Công an tỉnh; các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; Đội ứng cứu sự cố an ninh mạng của tỉnh.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm An ninh mạng quốc gia); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hằng năm.

IV. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch này được sử dụng từ nguồn ngân sách nhà nước theo phân cấp ngân sách hiện hành; lồng ghép với kinh phí thực hiện các chương trình, kế hoạch, đề án khác có liên quan và các nguồn kinh phí khác theo quy định của pháp luật.

V. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành cấp tỉnh, UBND các phường, xã

- Phân công lãnh đạo phụ trách, thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về ATTT mạng tại cơ quan, đơn vị, địa phương theo thẩm quyền quản lý.

- Thực hiện bố trí cán bộ, công chức, viên chức chuyên trách ATTT mạng tại cơ quan, đơn vị, địa phương mình; kịp thời thông báo về Công an tỉnh khi có sự thay đổi cán bộ, công chức, viên chức chuyên trách về ATTT mạng tại cơ quan, đơn vị hoặc đang là thành viên tham gia Đội ứng cứu sự cố an ninh mạng tỉnh.

- Xây dựng nội dung, lập dự toán kinh phí thực hiện các nhiệm vụ về ứng phó sự cố, bảo đảm ATTT mạng tại cơ quan, đơn vị, địa phương.

ng

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn HTTT theo quy định tại Điều 14 và Điều 15 Nghị định số 85/2016/NĐCP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ.

- Định kỳ 06 tháng và 01 năm, hoặc đột xuất báo cáo tình hình ứng phó sự cố, bảo đảm ATTT mạng tại cơ quan, đơn vị, địa phương về Công an tỉnh để tổng hợp báo cáo các cơ quan cấp trên theo quy định.

- Cử cán bộ, công chức tham gia các khóa đào tạo, tập huấn, diễn tập ứng phó sự cố của tỉnh để nâng cao kỹ năng và công tác tham mưu triển khai giám sát, bảo đảm ATTT mạng.

- Triển khai tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn, các hoạt động liên quan đến bảo đảm ATTT mạng của tỉnh, của cơ quan đơn vị trên Cổng, Trang thông tin điện tử, các phương tiện thông tin đại chúng: nội dung của Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP; Thông tư số 12/2022/TT-BTTTT; các Công điện, Chỉ thị của Thủ tướng Chính phủ và các Chỉ thị, văn bản của Bộ Thông tin và Truyền thông...

- Tích cực phối hợp với cơ quan, đơn vị chủ trì thực hiện các nhiệm vụ được giao theo Kế hoạch này. Căn cứ nội dung Kế hoạch và tình hình thực tế tại cơ quan, đơn vị, địa phương xây dựng, ban hành Kế hoạch ứng phó sự cố, bảo đảm ATTT mạng theo thẩm quyền quản lý và tổ chức triển khai các nhiệm vụ về ứng phó sự cố, bảo đảm ATTT mạng theo đúng tiến độ, chất lượng, hiệu quả.

2. Công an tỉnh

- Là cơ quan đầu mối, chuyên trách về ứng cứu sự cố ATTT mạng trên địa bàn tỉnh, có trách nhiệm chủ trì theo dõi, đôn đốc, phối hợp với các sở, ban, ngành, UBND các xã, phường tổ chức triển khai thực hiện Kế hoạch này. Định kỳ 06 tháng, 01 năm hoặc đột xuất tổng hợp báo cáo kết quả thực hiện gửi UBND tỉnh, Trung tâm An ninh mạng quốc gia để theo dõi, chỉ đạo.

- Hằng năm, tham mưu UBND tỉnh ban hành quyết định kiện toàn Đội ứng cứu sự cố an ninh mạng (nếu có thay đổi thành viên) để phù hợp với tình hình bảo đảm ATTT trên địa bàn tỉnh.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm ATTT định kỳ hằng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước, doanh nghiệp trên địa bàn tỉnh. Tiến hành xử lý theo quy định của pháp luật các cá nhân, cơ quan vi phạm trong công tác bảo đảm ATTT mạng.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn HTTT theo thẩm quyền quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của đơn vị chuyên trách ứng cứu sự cố và Đội ứng cứu sự cố an ninh mạng của tỉnh.

3. Sở Khoa học và Công nghệ

- Tổ chức triển khai, xây dựng, quản lý, vận hành hạ tầng mạng truyền số liệu dùng chung, kho dữ liệu tỉnh Nghệ An (data.nghean.gov.vn) và các hệ thống dùng chung được UBND tỉnh giao chủ trì triển khai; phối hợp Công an tỉnh trong thực hiện công tác bảo đảm ATTT đối với HTTT tập trung, dùng chung của tỉnh.

- Cử cán bộ có trình độ, kinh nghiệm tham gia xử lý, ứng cứu các sự cố về An ninh mạng, ATTT xảy ra trên địa bàn tỉnh khi có yêu cầu của đơn vị điều phối.

- Trao đổi kịp thời cho Công an tỉnh mọi thông tin liên quan đến các sự cố gây mất An ninh mạng, ATTT đối với HTTT tập trung, dùng chung của tỉnh.

4. Sở Tài chính

- Căn cứ khả năng cân đối ngân sách tỉnh, chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tham mưu bố trí kinh phí thực hiện Kế hoạch theo quy định của Luật Ngân sách nhà nước và các văn bản hướng dẫn có liên quan.

- Hướng dẫn, kiểm tra thực hiện nhiệm vụ, dự án hoặc các chương trình, Kế hoạch hằng năm của tỉnh về công tác ứng phó sự cố, bảo đảm ATTT mạng có sử dụng nguồn đầu tư công theo đúng quy định pháp luật hiện hành.

Yêu cầu các sở, ban, ngành cấp tỉnh; UBND các phường, xã triển khai thực hiện nghiêm túc; quá trình thực hiện có khó khăn, vướng mắc báo cáo UBND tỉnh (qua Công an tỉnh) để hướng dẫn, chỉ đạo. /

Nơi nhận:

- Trung tâm An ninh mạng quốc gia (để b/c);
- Chủ tịch, các PCT UBND tỉnh;
- Phó Chủ tịch TT UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- Chánh VP, các PVP UBND tỉnh;
- Công Thông tin điện tử tỉnh;
- UBND các phường, xã;
- Lưu: VT, NC (TP, Vinh).

✓

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH



Bùi Thanh An

