ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 95 /KH-UBND	*Hưng Yên, ngày 22 tháng 10 năm 2025*

KẾ HOẠCH
Ứng phó sự cố an toàn thông tin mạng trên địa bàn tỉnh Hưng Yên

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ 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;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) 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 hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 1622/QĐ-TTg ngày 25/10/2017 của Thủ tướng Chính phủ phê duyệt Đề án Đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ đến năm 2020, định hướng đến năm 2025;

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 không gian mạng đến năm 2025, tầm nhìn 2030;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng chống phần mềm độc hại;

Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ 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;

Căn cứ Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng;

Ủy ban nhân dân tỉnh Hưng Yên ban hành Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh, như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn tỉnh. Nghiên cứu, thu thập, xác minh, đánh giá, cảnh báo về sự cố, rủi ro an toàn thông tin mạng và phần mềm độc hại. Điều tra, phân tích các hoạt động an toàn thông tin liên quan đến tình huống, sự cố an toàn thông tin mạng nhằm nhanh chóng khôi phục hoạt động, giảm thiệt hại; đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an ninh mạng, an toàn thông tin đối với cán bộ, công chức, viên chức trong các cơ quan nhà nước của tỉnh.

- Xây dựng, phát triển Đội ứng cứu sự cố an toàn thông tin mạng có đầy đủ kiến thức, kỹ năng xử lý sự cố an toàn thông tin mạng đảm bảo linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- Đảm bảo 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 an toàn thông tin mạng.

2. Yêu cầu

- Các hệ thống thông tin của các cơ quan, đơn vị, địa phương phải được đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng; dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý.

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

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác đảm bảo an toàn thông tin giữa các cơ quan nhà nước trên địa bàn tỉnh; tăng cường sự phối hợp, hỗ trợ của cơ quan điều phối quốc gia về ứng cứu sự cố (VNCERT).

- Tham gia thường xuyên, đầy đủ các chương trình diễn tập tình huống hoặc thực chiến về ứng cứu sự cố an toàn thông tin mạng do các cơ quan chuyên trách tổ chức.

II. CÁC QUY ĐỊNH CHUNG

1. Phạm vi và đối tượng

Ứng phó sự cố an ninh mạng, an toàn thông tin đối với hệ thống thông tin các cơ quan, đơn vị, địa phương, tổ chức chính trị - xã hội trên địa bàn tỉnh Hưng Yên.

2. Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an ninh mạng, an toàn thông tin 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 hệ thống thông tin.

- 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 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.

3. Các lực lượng tham gia ứng phó sự cố

- Chủ quản hệ thống thông tin; đơn vị quản lý, vận hành hệ thống thông tin.

- Các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; các cơ quan, đơn vị, doanh nghiệp có liên quan.

- Đội Ứng cứu sự cố an ninh mạng tỉnh Hưng Yên (cơ quan Thường trực là Công an tỉnh).

- Doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng.

- Mời các cơ quan chuyên trách của các bộ, ngành có chức năng ứng cứu sự cố an ninh mạng, an toàn thông tin mạng 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 về an toàn thông tin mạng của tỉnh Hưng Yên (theo Quyết định số 332/QĐ-UBND ngày 18/7/2025 của UBND tỉnh) có trách nhiệm thực hiện tổ chức triển khai hoạt động ứng phó sự cố an toàn thông tin mạng đầy đủ, kịp thời theo quy định tại Quyết định số 05/2017/QĐ-TTg, Thông tư số 20/2017/TT-BTTTT và các và các nhiệm vụ khác khi xảy ra sự cố.

- Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh: Lực lượng chính tham gia các hoạt động ứng cứu sự cố an toàn thông tin mạng; thực hiện nhiệm vụ theo Quy chế hoạt động của Đội; tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia khi có yêu cầu từ Trung tâm Ứng cứu khẩn cấp không gian mạng hoặc các bộ, ngành có liên quan.

- Trung tâm Dữ liệu và Chuyển đổi số (thuộc Sở Khoa học và Công nghệ): Chịu trách nhiệm xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng, quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu; tham gia Đội ứng cứu sự cố an ninh mạng của tỉnh; xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn tỉnh Hưng Yên khi có yêu cầu của đơn vị điều phối.

- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh có trách nhiệm tổ chức quản lý, triển khai giám sát an toàn thông tin, cảnh báo về an toàn thông tin; là đầu mối điều phối kỹ thuật để xử lý thông tin vi phạm pháp luật trên không gian mạng theo quy định của pháp luật; tổ chức triển khai, kết nối chia sẻ thông tin với Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

- Các cơ quan, đơn vị, địa phương: Có trách nhiệm cử cán bộ, công chức, viên chức phụ trách, theo dõi công tác bảo đảm an toàn thông tin của đơn vị tham gia Đội ứng cứu sự cố an ninh mạng của tỉnh; phối hợp với đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng của tỉnh trong công tác ứng phó, xử lý các sự cố.

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

III. NỘI DUNG THỰC HIỆN

1. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

1.1. Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động 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 đơn vị cung cấp dịch vụ nếu có).

- Đơn vị chủ trì: Đơn vị quản lý, vận hành hệ thống thông tin.

- Đơn vị phối hợp: Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh; Trung tâm Dữ liệu và Chuyển đổi số, Sở Khoa học và Công nghệ; các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (trường hợp thuê dịch vụ) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

1.2. Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng bảo mật đối với các hệ thống thông tin 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 hệ thống thông tin.

- Đơn vị phối hợp: Phòng An ninh mạng và phòng, chống tội phạm sử dụng

công nghệ cao, Công an tỉnh; Trung tâm Dữ liệu và Chuyển đổi số, Sở Khoa học và Công nghệ; các doanh nghiệp cung cấp dịch vụ an toàn thông tin 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 hệ thống thông tin, chương trình ứng dụng, các cơ quan, đơn vị, địa phương 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 bảo đảm các nội dung:

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

+ 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 an toàn thông tin mạng khác.

Phương án đối phó, khắc phục sự cố đối với một hoặc nhiều tình huống

- 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;

+ 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 hệ thống thông tin;

+ 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 an toàn thông tin;

+ 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 thiên tai, thảm họa tự nhiên, như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất an toàn thông tin mạng khác.

Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, 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: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; Đội ứng cứu sự cố an ninh mạng tỉnh Hưng Yên; Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh; Trung tâm Dữ liệu và Chuyển đổi số, Sở Khoa học và Công nghệ; Doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

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 cơ quan, đơn vị, địa phương trên địa bàn tỉnh.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu sự cố an ninh mạng của tỉnh; Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh; Trung tâm Dữ liệu và Chuyển đổi số, Sở Khoa học và Công nghệ; Doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

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

3.1. Báo cáo sự cố an toàn thông tin mạng theo quy định tại Điều 11, Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ, Điều 9 Thông tư số 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Đơn vị thực hiện:

+ Đơn vị quản lý, vận hành hệ thống thông tin báo cáo cơ quan Chủ quản hệ thống thông tin, Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh (qua Phòng

An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh); đồng gửi Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

+ Công an tỉnh báo cáo Chủ tịch UBND tỉnh, Cơ quan điều phối quốc gia và báo cáo Cơ quan thường trực và Ban Chỉ đạo quốc gia về ứng cứu sự cố.

- 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 an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 10 Thông tư 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Đơn vị chủ trì: Công an tỉnh; Đơn vị quản lý, vận hành hệ thống thông tin (các cơ quan, đơn vị); Đội Ứng cứu sự cố an ninh mạng của tỉnh.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị chức năng 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 an toàn thông tin 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 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Đơn vị chủ trì: Đội Ứng cứu sự cố an ninh mạng tỉnh Hưng Yên.

- Đơn vị phối hợp: Các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; Đơn vị quản lý, vận hành hệ thống thông tin.

- Thời gian thực hiện: Thường xuyên.

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 (nay là Bộ Khoa học và Công nghệ) về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng, bao gồm:

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

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: Đội ứng cứu sự cố an toàn thông tin của tỉnh; Công an tỉnh; Sở Khoa học và Công nghệ.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; Doanh nghiệp cung cấp dịch vụ an toàn thông tin (nếu có); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

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

Thực hiện nghiêm công tác giám sát, phát hiện sớm nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin 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 an toàn thông tin mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; 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 hệ thống thông tin; Đội ứng cứu sự cố an ninh mạng mạng của tỉnh.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Thường xuyên.

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

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 phối hợp các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường.

- Đơn vị phối hợp: Doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

IV. KINH PHÍ THỰC HIỆN

- Kinh phí thực hiện Kế hoạch được bố trí từ nguồn ngân sách hằng năm của tỉnh bảo đảm cho hoạt động ứng phó sự cố an ninh mạng, an toàn thông tin và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

- Chủ quản hệ thống thông tin phải bố trí kinh phí để thực hiện Kế hoạch, phương án ứng cứu sự cố, dự phòng kinh phí xử lý sự cố, khắc phục hậu quả, khôi phục dữ liệu và hoạt động bình thường của hệ thống thông tin của mình.

V. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành, đoàn thể; UBND các xã, phường

- Căn cứ nội dung Kế hoạch này và tình hình thực tế tại cơ quan, đơn vị, địa phương xây dựng, ban hành Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng, nội dung theo hướng dẫn tại Phụ lục 3 của Thông tư 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) theo thẩm quyền quản lý và tổ chức triển khai các nhiệm vụ về ứng phó sự cố, bảo đảm an toàn thông tin mạng theo đúng tiến độ, chất lượng, hiệu quả.

- Ưu tiên bố trí nguồn lực *(nhân lực, kinh phí)* và điều kiện để triển khai hoạt động ứng cứu sự cố an ninh mạng, an toàn thông tin trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý. Xây dựng nội dung, lập dự toán kinh phí thực hiện các nhiệm vụ về ứng phó sự cố, bảo đảm an toàn thông tin mạng của cơ quan, đơn vị mình hàng năm để tổ chức triển khai thực hiện, tránh chồng chéo, lãng phí.

- Phân công lãnh đạo phụ trách; thành lập hoặc chỉ định bộ phận đầu mối; bố trí cán bộ, công chức, viên chức chuyên trách thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin tại cơ quan, đơn vị trong phạm vi quản lý. Hằng quý hoặc khi có sự thay đổi cán bộ, công chức, viên chức chuyên trách về an toàn thông tin mạng tại cơ quan, đơn vị hoặc đang là thành viên tham gia Đội Ứng cứu sự cố an ninh mạng của tỉnh thì đơn vị kịp thời thông báo về Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh *(cung cấp đầy đủ các thông tin, gồm: Họ và tên; Cấp bậc; Chức vụ; Đơn vị công tác; Số điện thoại; Email,...)*

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Điều 13, Điều 14 và Điều 15 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Định kỳ (06 tháng, 01 năm) hoặc đột xuất, các đơn vị báo cáo tình hình ứng phó sự cố, bảo đảm an ninh mạng, an toàn thông tin trong phạm vi quản lý để tổng hợp báo cáo cấp trên theo quy định.

- Cử cán bộ tham gia đầy đủ các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về ứng cứu sự cố, bảo đảm an toàn thông tin mạng để nâng cao kỹ năng và công tác tham mưu, triển khai giám sát, bảo đảm an toàn thông tin mạng.

- 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 hoạt động ứng cứu sự cố an

toàn thông tin, đảm bảo an ninh mạng, an toàn thông tin trên các Trang/Cổng thông tin điện tử, các phương tiện thông tin đại chúng…

2. Công an tỉnh

- Tham mưu, trình Chủ tịch Ủy ban nhân dân tỉnh ban hành Quyết định thành lập, kiện toàn Đội Ứng cứu sự cố an ninh mạng tỉnh Hưng Yên.

- Thực hiện trách nhiệm, quyền hạn của đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng theo Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) và Quyết định số 332/QĐ-UBND ngày 18/7/2025 của Ủy ban nhân dân tỉnh Hưng Yên.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm an toàn thông tin định kỳ hàng năm hoặc theo chỉ đạo của Chủ tịch UBND tỉnh đối với các cơ quan nhà nước trên địa bàn tỉnh.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo thẩm quyền quy định tại khoản 1, 2 Điều 12, khoản 5 Điều 15 của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và hướng dẫn tại Thông tư số 12/2022/TT- BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Định kỳ (06 tháng, 01 năm) hoặc đột xuất, tổng hợp báo cáo kết quả thực hiện ứng phó sự cố, bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh gửi Chủ tịch UBND tỉnh, Bộ Công an theo quy định.

- Phối hợp các đơn vị có liên quan tổ chức tuyên truyền các hoạt động ứng phó sự cố, bảo đảm an ninh mạng, an toàn thông tin trên các trang/cổng thông tin điện tử của tỉnh, các fanpage, blog, diễn đàn,…

- Nghiên cứu, thiết lập kênh hotline 24/7 hỗ trợ ứng cứu sự cố an ninh mạng trên nền tảng ứng dụng bảo mật (Signet); hướng dẫn thành viên Đội Ứng cứu sự cố an ninh mạng tỉnh tham gia.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của 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, trung tâm dữ liệu, hạ tầng, nền tảng, cơ sở dữ liệu dùng chung, phục vụ chuyển đổi số, ứng dụng công nghệ thông tin; phối hợp Công an tỉnh trong thực hiện công tác đảm bảo an toàn thông tin đối với hệ thống thông tin 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 toàn thông tin, an ninh mạng xảy ra trên địa bàn tỉnh Hưng Yên khi có yêu cầu của đơn vị điều phối.

- Phối hợp với Công an tỉnh trong công tác giám sát an toàn thông tin đối với hệ thống thông tin tại Trung tâm tích hợp dữ liệu; kịp thời trao đổi Công an tỉnh thông tin liên quan đến các sự cố gây mất an ninh mạng, an toàn thông tin đối với hệ thống thông tin tập trung, dùng chung của tỉnh.

- Phối hợp các cơ quan, đơn vị, địa phương triển khai thực hiện hiệu quả công tác tuyên truyền, phổ biến pháp luật về an toàn thông tin, an ninh mạng.

4. Sở Tài chính

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

5. Trong quá trình thực hiện nếu có khó khăn, vướng mắc, đề nghị các cơ quan, đơn vị, địa phương kịp thời trao đổi Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)* để báo cáo Chủ tịch Ủy ban nhân dân tỉnh có hướng chỉ đạo giải quyết, xử lý. Giao Công an tỉnh chủ trì, giúp Chủ tịch UBND tỉnh theo dõi, hướng dẫn, kiểm tra, đôn đốc việc thực hiện và tổng hợp báo cáo theo quy định./.

Nơi nhận:
- Trung tâm An ninh mạng Quốc gia; *(qua A05 - Bộ Công an)*
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành, đoàn thể;
- Lãnh đạo VP UBND tỉnh;
- UBND các xã, phường;
- Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet trên địa bàn tỉnh Hưng Yên;
- Lưu: VT, CVNC[Tường], CAT(PA05-Đ2).

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

ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN
ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN
22/10/2025 11:29:39

ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN

Nguyễn Lê Huy