ỦY BAN NHÂN DÂN TỈNH THÁI NGUYÊN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 2477 /QĐ-UBND	*Thái Nguyên, ngày 26 tháng 12 năm 2025*

QUYẾT ĐỊNH
Ban hành Phương án ứng phó sự cố an ninh mạng trên địa bàn tỉnh Thái Nguyên

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH THÁI NGUYÊN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16 tháng 6 năm 2025;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 06 năm 2006;

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

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 04 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của các cơ quan nhà nước;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ về quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 03 năm 2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 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;

Theo đề nghị của Giám đốc Công an tỉnh Thái Nguyên tại Tờ trình số 4336/TTr-CAT-PA05 ngày 17 tháng 12 năm 2025.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Phương án ứng phó sự cố an ninh mạng trên địa bàn tỉnh Thái Nguyên.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng UBND tỉnh; Giám đốc Công an tỉnh; Chỉ huy trưởng Bộ Chỉ huy Quân sự tỉnh; Giám đốc các sở, Thủ trưởng các ban, ngành thuộc UBND tỉnh; Chủ tịch UBND các xã, phường và các cơ quan, đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này.

Nơi nhận:
- Như Điều 3;
- Bộ Công an;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Lãnh đạo Văn phòng UBND tỉnh;
- Lưu: VT, NC.

Vandt

CHỦ TỊCH

Vương Quốc Tuấn

ỦY BAN NHÂN DÂN
TỈNH THÁI NGUYÊN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

PHƯƠNG ÁN
Ứng phó sự cố an ninh mạng trên địa bàn tỉnh Thái Nguyên

(Ban hành theo Quyết định số 2477 /QĐ-UBND ngày 26 tháng 12 năm 2025 của Chủ tịch UBND tỉnh Thái Nguyên)

I. MỤC TIÊU VÀ PHẠM VI ÁP DỤNG

1. Mục tiêu

Phương án ứng phó sự cố an ninh mạng được xây dựng nhằm:

- Chủ động phòng ngừa, phát hiện sớm, ứng phó kịp thời và khắc phục hậu quả của các sự cố an ninh mạng có thể xảy ra;

- Bảo đảm tính toàn vẹn, tính sẵn sàng và tính bảo mật của hệ thống thông tin, dữ liệu của tổ chức;

- Giảm thiểu tối đa thiệt hại và thời gian gián đoạn hoạt động khi xảy ra sự cố;

- Thiết lập cơ chế phối hợp chặt chẽ với lực lượng chuyên trách về an ninh mạng, phục vụ hoạt động điều tra, xử lý và khôi phục, nâng cao năng lực phản ứng nhanh, điều tra số và khôi phục sau sự cố;

- Tuân thủ các quy định pháp lý hiện hành về an ninh mạng, an toàn thông tin.

2. Phạm vi áp dụng

- Áp dụng cho toàn bộ hệ thống thông tin, dữ liệu, tài nguyên số, ứng dụng, thiết bị phần cứng và phần mềm thuộc quản lý của tổ chức;

- Áp dụng cho tất cả cán bộ, nhân viên, quản trị viên, nhà thầu và các bên liên quan có quyền truy cập hệ thống thông tin của tổ chức;

- Áp dụng đối với tất cả sự cố của Hệ thống thông tin (sau đây viết tắt là HTTT) ở mọi cấp độ, từ mức độ sự cố đơn lẻ đến sự cố quy mô lớn, có yếu tố phá hoại, gián điệp hoặc ảnh hưởng tới an ninh quốc gia;

- Áp dụng cho cả hệ thống tại chỗ và hệ thống đám mây, mạng riêng ảo (VPN), mạng diện rộng (WAN), thiết bị đầu cuối và hệ thống IoT nếu có;

- Phạm vi áp dụng còn bao gồm các đơn vị trực thuộc, chi nhánh, văn phòng đại diện hoặc tổ chức liên kết đang sử dụng chung hạ tầng HTTT với đơn vị chủ quản.

II. THÀNH PHẦN VÀ ĐẦU MỐI ỨNG CỨU SỰ CỐ

Tổ chức ứng cứu sự cố tại đơn vị bao gồm: Đội ứng cứu sự cố (sau đây viết tắt là Đội ƯCSC) an ninh mạng nội bộ của đơn vị chủ quản, các bộ phận liên quan; Đội

ƯCSC an ninh mạng tỉnh Thái Nguyên; Lực lượng chuyên trách đảm bảo an ninh mạng tại địa phương (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh Thái Nguyên).

1. Thành lập Đội ứng cứu sự cố nội bộ

Chủ quản HTTT thành lập Đội ƯCSC an ninh mạng nội bộ để thực hiện nhiệm vụ phát hiện, xử lý, phối hợp và khắc phục sự cố an toàn thông tin trong phạm vi sự cố. Đội ƯCSC có thể bao gồm đại diện từ các bộ phận sau: Công nghệ thông tin, An toàn thông tin, Quản trị hệ thống, Quản lý vận hành, Pháp chế, Truyền thông hoặc cán bộ phụ trách xử lý rủi ro (nếu cần).

Đội ƯCSC hoạt động theo quy chế phối hợp nội bộ, chịu sự chỉ đạo chung của lãnh đạo đơn vị và phối hợp chặt chẽ với đầu mối điều phối ứng cứu.

Đơn vị chỉ định rõ ràng đầu mối phục vụ điều phối ứng cứu sự cố là cá nhân hoặc bộ phận chịu trách nhiệm: (1) Tiếp nhận thông tin về sự cố từ hệ thống giám sát, người dùng hoặc cảnh báo từ bên ngoài; (2) Kích hoạt quy trình ứng cứu, phân công nhiệm vụ và tổ chức triển khai biện pháp xử lý ban đầu; (3) Báo cáo cho Công an tỉnh (Cơ quan chuyên trách về An toàn thông tin mạng tỉnh, qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) và làm đầu mối liên hệ với các cơ quan chuyên trách về an ninh mạng; (4) Tổng hợp, báo cáo và cập nhật diễn biến sự cố theo đúng quy định; (5) Làm đầu mối phối hợp với các doanh nghiệp cung cấp dịch vụ an toàn thông tin (nếu được huy động).

Trong trường hợp sự cố an ninh mạng có thể gây ảnh hưởng đến xã hội, yếu tố về truyền thông cần được tính toán kỹ lưỡng và có thể cần thông qua của nhiều cấp để giảm thiểu các rủi ro.

2. Trách nhiệm của các bộ phận liên quan

Các đơn vị, bộ phận hoặc cá nhân có liên quan đến HTTT tại đơn vị hoặc các doanh nghiệp điều phối ứng cứu sự cố có trách nhiệm: (1) Phối hợp với đầu mối điều phối và Đội ƯCSC trong quá trình phát hiện, phân tích, cô lập và khắc phục sự cố; (2) Cung cấp đầy đủ, kịp thời thông tin, nhật ký hệ thống, dữ liệu kỹ thuật, và các yếu tố liên quan phục vụ điều tra nguyên nhân sự cố; (3) Thực hiện nghiêm túc yêu cầu kỹ thuật, nghiệp vụ, bảo toàn hiện trạng hệ thống khi có yêu cầu từ lực lượng chuyên trách về an ninh mạng hoặc cơ quan điều phối ứng cứu sự cố.

3. Đội ứng cứu sự cố an ninh mạng tại địa phương

Đội ƯCSC an ninh mạng tỉnh có trách nhiệm tiếp nhận và xử lý sự cố an ninh mạng đối với các sự cố mà Đội ƯCSC nội bộ không xử lý được hoặc khi được yêu cầu. Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh là đơn vị chủ trì tiếp nhận, điều phối hoạt động của Đội ƯCSC

Trong trường hợp không xử lý được, Đội ƯCSC địa phương thực hiện báo cáo cho Trung tâm An ninh mạng quốc gia để nhận sự hỗ trợ.

4. Lực lượng chuyên trách đảm bảo an ninh mạng ở địa phương

Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh có trách nhiệm tiếp nhận thông tin báo cáo sự cố an ninh mạng, phối hợp với các Đội ƯCSC nội bộ triển khai các công cụ và phương tiện cần thiết để thu thập chứng cứ số, dữ liệu để đánh giá thiệt hại theo các quy định của pháp luật (luật dữ liệu, luật bảo vệ dữ liệu cá nhân....) hướng dẫn các đơn vị xử lý sự cố đảm bảo theo yêu cầu pháp luật.

III. QUY TRÌNH ỨNG PHÓ SỰ CỐ

1. Phát hiện và báo cáo

Khi phát hiện dấu hiệu bất thường trong hệ thống (thông qua giám sát, cảnh báo kỹ thuật hoặc phản ánh từ người dùng...), chủ quản HTTT phải kịp thời kích hoạt quy trình ứng phó sự cố. Toàn bộ cán bộ, nhân viên có trách nhiệm thông báo sự cố tới đội quản trị hệ thống và Đội ƯCSC nội bộ (nếu đã được thành lập).

Đơn vị vận hành HTTT, đơn vị giám sát an ninh mạng có trách nhiệm báo cáo sự cố tới cơ quan chủ quản, đơn vị chuyên trách ứng cứu sự cố cùng cấp chậm nhất 12 giờ kể từ khi phát hiện sự cố (thời hạn này có thể thay đổi tùy thuộc vào điều khoản của hợp đồng trong trường hợp sử dụng các nhà cung cấp dịch vụ nhưng không được quá 12 giờ).

Chủ quản HTTT bắt buộc phải thực hiện báo cáo khẩn cấp tới Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) trong thời hạn không quá 24 giờ kể từ thời điểm tiếp nhận thông tin hoặc phát hiện sự cố, thông qua các kênh được chỉ định (email chính thức, cổng tiếp nhận báo cáo, hotline trực 24/7); khai báo trên Hệ thống Điều hành an ninh mạng quốc gia (soar.soc.gov.vn), Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh là đơn vị thực hiện khai báo trong trường hợp chưa cấp tài khoản cho chủ quản HTTT.

Báo cáo sự cố phải được thực hiện ngay lập tức và được duy trì trong suốt quá trình ứng cứu sự cố gồm: Báo cáo ban đầu; báo cáo diễn biến tình hình; báo cáo phương án ứng cứu cụ thể; báo cáo xin ý kiến chỉ đạo, chỉ huy; báo cáo đề nghị hỗ trợ, phối hợp; báo cáo kết thúc ứng phó.

Nội dung báo cáo cần bao gồm Tên, địa chỉ Đơn vị vận hành HTTT; cơ quan chủ quản HTTT; HTTT bị sự cố; thời điểm phát hiện sự cố; Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố; Mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức; Đơn vị cung cấp dịch vụ hạ tầng công nghệ thông tin,

viễn thông; Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố; Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo; Kết quả ứng cứu sự cố ban đầu; Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có).

2. Ứng phó ban đầu

Ngay sau khi phát hiện sự cố, chủ quản HTTT (Đội ƯCSC nội bộ) có trách nhiệm tiến hành ứng phó ban đầu nhằm hạn chế mức độ ảnh hưởng và cô lập khu vực bị tác động, đồng thời giữ nguyên hiện trạng hệ thống và thực hiện theo hướng dẫn của Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh để phục vụ công tác điều tra (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao có trách nhiệm yêu cầu thực hiện việc này đối với các sự cố nghi ngờ do tấn công mạng). Các hành động ưu tiên bao gồm: cách ly hệ thống bị ảnh hưởng bằng cách ngắt kết nối mạng (nhưng không tắt nguồn hoặc khởi động lại thiết bị); Ghi nhận các thông tin tại thời điểm xảy ra sự cố (tiến trình đang chạy, kết nối mạng, IP truy cập...); Sao lưu nhật ký hệ thống (log), các file nghi ngờ, ảnh ổ đĩa, dữ liệu RAM theo đúng quy trình pháp y số.

Đối với hệ thống không thể cách ly hoàn toàn, tìm các phương án chặn lọc kết nối của hệ thống với các IP nghi ngờ là độc hại.

Trường hợp cần duy trì và khôi phục hoạt động của hệ thống bị ảnh hưởng, tiến hành việc chuyển sang hệ thống dự phòng hoặc khôi phục trên hạ tầng mới từ các bản sao lưu.

Trong trường hợp nghi ngờ có yếu tố tấn công có chủ đích hoặc không đủ năng lực tự xử lý, chủ quản HTTT phải đề nghị lực lượng chuyên trách về an ninh mạng trực tiếp phối hợp điều tra, hoặc chủ trì điều phối các doanh nghiệp an toàn thông tin chuyên nghiệp hỗ trợ xử lý. Khi đó, Công an tỉnh triệu tập Đội ƯCSC địa phương để hỗ trợ chủ quản xử lý sự cố.

Trong quá trình xử lý sự cố, tăng cường việc giám sát an ninh mạng để phát hiện các hành vi tấn công mạng khác vào hệ thống, điều chỉnh phạm vi ảnh hưởng và kiểm tra hiệu quả của các biện pháp ngăn chặn đã thực hiện.

3. Phân tích và đánh giá mức độ nghiêm trọng

Ngay sau khi thực hiện các biện pháp ứng phó ban đầu, đội ngũ kỹ thuật và lực lượng chuyên trách sẽ tiến hành đánh giá sơ bộ và phân loại mức độ nghiêm trọng của sự cố:

Mức 1: Phạm vi ảnh hưởng cục bộ, hệ thống vẫn có thể cung cấp dịch vụ, không có dữ liệu nhạy cảm bị truy cập – chủ quản HTTT có thể xử lý nội bộ, thực hiện khắc phục theo quy trình sẵn có, thu thập dữ liệu theo yêu cầu của Phòng An ninh

mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh và gửi báo cáo tổng kết kèm dữ liệu theo yêu cầu cho lực lượng chuyên trách sau khi hoàn tất.

Mức 2: Ảnh hưởng trung bình, có gián đoạn cục bộ, nguy cơ rò rỉ dữ liệu người dùng hoặc chưa xác định rõ toàn bộ vùng bị tác động – chủ quản HTTT phải phối hợp chặt chẽ với lực lượng chuyên trách để đánh giá hiện trạng và xác lập phạm vi ảnh hưởng. Trong trường hợp cần thiết, lực lượng chuyên trách có thể xem xét huy động sự hỗ trợ kỹ thuật từ doanh nghiệp an toàn thông tin nhằm hỗ trợ khoanh vùng, loại bỏ nguyên nhân và phục hồi hệ thống trong thời gian sớm nhất.

Mức 3: Sự cố nghiêm trọng, có dấu hiệu phá hoại, lộ lọt tài liệu nội bộ, nhạy cảm, tấn công có chủ đích hoặc phạm vi ảnh hưởng vượt quá khả năng kiểm soát của chủ quản HTTT – lực lượng chuyên trách về an ninh mạng giữ vai trò điều phối chính trong toàn bộ quá trình ứng phó, điều tra và khắc phục sự cố. Tùy theo tình hình cụ thể, lực lượng chuyên trách có thể triển khai các biện pháp kỹ thuật trực tiếp, đồng thời huy động lực lượng từ các doanh nghiệp cung cấp dịch vụ ATTT phù hợp để hỗ trợ khôi phục hệ thống trong thời gian ngắn nhất, đảm bảo duy trì hoạt động tối thiểu và giảm thiểu thiệt hại.

4. Thu thập dữ liệu, điều tra nguyên nhân sự cố

Đơn vị chủ quản HTTT và các doanh nghiệp được mời tham gia xử lý, khắc phục sự cố có trách nhiệm phối hợp chặt chẽ, cung cấp đầy đủ thông tin, tuân thủ các yêu cầu nghiệp vụ và kỹ thuật do lực lượng chuyên trách chỉ định, bao gồm cả việc bảo toàn hiện trạng phục vụ điều tra, hỗ trợ thu thập chứng cứ điện tử, cũng như triển khai các giải pháp phòng ngừa nguy cơ tái xâm nhập sau khi phục hồi.

Xác định nguyên nhân sự cố là yêu cầu quan trọng của quá trình xử lý để khắc phục triệt để các yếu điểm gây ra sự việc. Các đơn vị theo phân công và trách nhiệm phân tích dữ liệu, thực hiện thêm các biện pháp kiểm thử (pentest) trong trường hợp cần thiết để xác định rõ nguyên nhân.

5. Làm sạch và phục hồi

Mục tiêu của giai đoạn này là loại bỏ hoàn toàn nguyên nhân sự cố, phục hồi hệ thống và đảm bảo an toàn khi vận hành trở lại. Các biện pháp xử lý có thể bao gồm: Gỡ bỏ mã độc, đóng các cổng dịch vụ bị khai thác, vá lỗ hổng, đổi mật khẩu, thu hồi tài khoản bị xâm nhập, cập nhật chính sách phân quyền, cấu hình lại hệ thống bảo mật. Hệ thống cần được phục hồi từ bản sao lưu sạch đã được kiểm tra tính toàn vẹn, tránh trường hợp khôi phục từ bản sao đã bị nhiễm mã độc. Trước khi đưa hệ thống trở lại hoạt động chính thức, chủ quản HTTT phải thực hiện các bước kiểm tra độc lập, thử nghiệm kỹ thuật và tăng cường giám sát sau khôi phục.

Lực lượng chuyên trách về an ninh mạng có trách nhiệm thực hiện công tác điều tra và xác minh trên cơ sở các dữ liệu, chứng cứ điện tử do chủ quản HTTT cung cấp hoặc thu thập được trong quá trình xử lý sự cố; thực hiện xử lý theo quy định

pháp luật trong trường hợp phát hiện dấu hiệu vi phạm; thực hiện đánh giá các yếu tố khác liên quan đến quy định của pháp luật (dữ liệu, bí mật nhà nước, dữ liệu cá nhân, kinh tế, xã hội...)

Ngoài ra, lực lượng chuyên trách cần hướng dẫn chủ quản HTTT bị ảnh hưởng triển khai biện pháp kỹ thuật tạm thời, hỗ trợ đảm bảo hoạt động tối thiểu, đồng thời đề xuất các khuyến nghị nâng cao năng lực phòng thủ cho chủ quản HTTT sau khi sự cố được kiểm soát.

6. Báo cáo hoàn tất và rút kinh nghiệm

Sau khi sự cố đã được xử lý và hệ thống đi vào vận hành ổn định, chủ quản HTTT có trách nhiệm hoàn thiện báo cáo kết quả xử lý sự cố gửi về lực lượng chuyên trách an ninh mạng. Báo cáo cần nêu rõ nguyên nhân, quy trình xử lý, các biện pháp đã triển khai, đánh giá thiệt hại và đề xuất khuyến nghị phòng ngừa. Đồng thời, chủ quản HTTT phải tiến hành rút kinh nghiệm nội bộ, cập nhật quy trình ứng phó, điều chỉnh chính sách an toàn thông tin, bổ sung công cụ giám sát, khắc phục các lỗ hổng bảo mật và tổ chức tập huấn lại cho các bộ phận liên quan. Hồ sơ sự cố phải được lưu trữ đầy đủ, có chữ ký xác nhận, và bảo quản trong thời gian tối thiểu ba năm để phục vụ thanh tra, kiểm tra khi cần thiết.

Căn cứ phương án này, các cơ quan, đơn vị, địa phương xây dựng kịch bản ứng phó sự cố an ninh mạng cho các hệ thống, ưu tiên các HTTT quan trọng và các loại sự cố an ninh mạng ảnh hưởng đến các yếu tố quan trọng của hệ thống (ví dụ ransomware; lộ lọt dữ liệu đối với các hệ thống văn bản quan trọng, lưu trữ dữ liệu cá nhân; deface đối với các cổng thông tin;...).

Trên đây là Phương án ứng phó sự cố an ninh mạng trên địa bàn tỉnh Thái Nguyên. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các đơn vị, địa phương báo cáo UBND tỉnh *(qua Công an tỉnh tổng hợp)* để kịp thời xem xét, giải quyết./.